Sensitive Security Information, Certified® (SSI) Body of Knowledge

Recommended Reading for Sensitive Security Information Certified®

American Board for Certification in Homeland Security

CRC Press
Taylor & Francis Group

Sensitive Security Information, Certified® (SSI) Body of Knowledge

Center for National Threat Assessment

Certified Forensic Consultant Body of Knowledge
American College of Forensic Examiners Institute
ISBN: 978-1-4987-5207-7

The Certified Criminal Investigator Body of Knowledge
American College of Forensic Examiners Institute
ISBN: 978-1-4987-5205-3

Sensitive Security Information, Certified® (SSI) Body of Knowledge
American Board for Certification in Homeland Security
ISBN: 978-1-4987-5211-4

Sensitive Security Information, Certified® (SSI) Body of Knowledge

American Board for Certification in Homeland Security

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2016 by American Board for Certification in Homeland Security
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20160129

International Standard Book Number-13: 978-1-4987-5213-8 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Part I Perspective

Chapter 1 The History of SSI 3
1.1 The Context of Sensitive Security Information (SSI) 3
1.1.1 First Use of the Term *SSI* 3
1.1.2 Effects of 9/11 3
1.2 Defining SSI 4
1.2.1 Early Definitions 4
1.2.2 Current Definition 4
1.2.3 Designating SSI 5
1.3 Securing SSI 6
Bibliography 6

Chapter 2 Terms and Definitions 9
2.1 Government Information 9
2.1.1 Confidential Classification 9
2.1.1.1 Sensitive Security Information (SSI) Recap 10
2.1.2 Secret Classification 10
2.1.3 Top Secret 10
2.2 Public Information 10
2.2.1 Trade Secrets 11
2.2.2 Information Theft 12
2.3 Personal Information 12
2.3.1 Responsibility of Secrecy 12
2.3.2 Breaches in Personal Information 13

2.4 Sensitive but Unclassified (SBU) Information 13
2.4.1 SSI Designation 13
2.4.2 SBU Designations 14
Bibliography 16

CHAPTER 3 THE IMPORTANCE OF SSI 17
3.1 Dangers to Sensitive Information 17
3.1.1 Trust 17
3.1.2 Complacency 18
3.1.3 Espionage 19
3.2 Thwarting Economic Espionage 22
3.2.1 Creating Spy Networks 22
3.2.2 Acquiring Trade Secrets 22
3.2.3 Protecting against Espionage 23
3.3 Sensitive Information and Where It Exists 23
3.3.1 Types of Sensitive Information 23
3.3.2 Sensitive Information Locations 24
3.3.3 Overlooked Sources of Sensitive Information 25
3.4 Identifying Computer Vulnerabilities 27
3.5 Domestic Economic Espionage 27
3.5.1 On-the-Ground Intelligence 28
3.5.2 Computer Hackers 29
Bibliography 30

CHAPTER 4 THE HISTORY OF THE SSI CLASSIFICATION SYSTEM 31
4.1 1951: Executive Order 10290 31
4.2 1953: EO 10501 31
4.3 1966: Freedom of Information Act 32
4.4 1974: The Privacy Act 32
4.5 1977: Presidential Directive (PD/NSC-24) 33
4.6 1985: National Security Decision Directive 33
4.7 1987: Computer Security Act 33
4.8 1992: "CIA Openness" 34
4.9 1995: EO 12958 34
4.10 2002: The Card Memorandum 34
4.11 2003: EO 13292 35
4.12 2005: SBU Information Memorandum 35
Bibliography 36

PART II ESPIONAGE AND SECURITY BREACHES

CHAPTER 5 THE HISTORY OF SPIES AND ESPIONAGE 39
5.1 Espionage in Ancient Times 39
5.1.1 The Bible 40
5.1.2 496 BC 40
5.1.3 334 BC 41

5.1.4 350–280 BC 41
5.1.5 c. 300 BC 41
5.1.6 50(s) BC 41
5.1.7 44 BC 42
5.2 Espionage: Ninth Century AD–Eighteenth Century AD 42
5.2.1 Ninth Century AD 42
5.2.2 AD 54 42
5.2.3 AD 240–320 42
5.2.4 AD 878 42
5.2.5 1300s 42
5.2.6 1420s 43
5.2.7 1424 43
5.2.8 1450 43
5.2.9 1558–1663 43
5.2.10 Late 1600s–Early 1700s 44
5.3 Pre–20th-Century Events 44
5.3.1 Daniel Defoe, Born 1660 44
5.3.2 The 1700s and the American Revolutionary War 44
5.4 The Revolutionary War 46
5.4.1 The Culper Gang 47
5.4.2 Nathan Hale 47
5.4.3 Committee of Secret Correspondence 48
5.4.4 Benedict Arnold 48
5.4.5 Joseph Fouché, Duc d'Otrante, Born c. 1759 49
5.4.6 Prince Clemens von Metternich, Born 1773 49
5.5 The 1800s: New Inventions 49
5.5.1 Pinkerton National Detective Agency, Founded 1850 50
5.5.2 Okhrana (Department for Defense of Public Security and Order), Formally Organized 1881 50
5.6 Civil War Spying 51
5.6.1 Harriet Tubman 52
5.6.2 Elizabeth Van Lew 52
5.6.3 Belle Boyd 53
5.6.4 Rose Greenhow 53
5.7 Early 20th Century 54
5.7.1 Mata Hari 54
5.7.2 Sidney Reilly 55
5.8 World War I: A Proving Ground for Espionage 56
5.8.1 Captain Franz von Rintelen 57
5.8.2 Carl Lody 57
5.8.3 Irving Guy Ries 58
5.8.4 Choctaw Code 58
5.9 Spies Helped Allies Win World War II 59
5.9.1 Navajo Code Talkers 60
5.9.2 Unusual Tactics 60
5.9.3 Takeo Yoshikawa, the Pearl Harbor Spy 60

5.9.4 Virginia Hall, "the Limping Lady" 61
5.9.5 The Dead Decoy 62
5.9.6 The Cambridge Spies 63
5.9.7 Gestapo, Formally Organized in 1933 64
5.9.8 British Double Agents during World War II, 1940–1945 65
5.9.9 Central Intelligence Agency (CIA), Formally Organized in 1947 65
5.10 The Cold War 65
5.10.1 Alger Hiss—Born in 1904, Trial in 1950 65
5.10.2 Julius and Ethel Rosenberg—Born in 1918 and in 1915, Respectively; Trial in 1951 66
5.10.3 Markus Wolf 67
5.10.4 Christopher Boyce—Born in 1953, Arrested in 1977; Andrew Lee—Born in 1952, Arrested in 1976 68
5.10.5 The Walker Spy Ring 68
5.10.6 Jonathan Pollard—Born in 1954, Plea Agreement in 1986 70
5.10.7 Colonel George Trofimoff 70
5.10.8 Aldrich Ames—Born in 1941, Arrested in 1994 73
5.10.9 Robert Hanssen 74
5.10.10 Wen Ho Lee 76
5.11 September 11, 2001, and Its Aftermath 80
5.11.1 The PATRIOT Act 80
5.11.2 United States Departments in Action 81
5.11.3 Weapons of Mass Destruction 82
5.12 Recent History—More Lapses in Security 83
5.12.1 Sandy Berger 83
5.12.2 Leandro Aragoncillo—Born in 1959, Indicted in 2005 84
Bibliography 85

CHAPTER 6 ESPIONAGE AND PSYCHOLOGY 89
JANET MIELKE SCHWARTZ, PhD, DABFE, DACFM, DABPS, FACE, CHS III
6.1 Development of the Office of Strategic Services 89
6.2 Mission and Purpose of the OSS 90
6.3 The Making of a World War II Spy 90
6.3.1 General Variables and Characteristics 90
6.3.2 The Recruiting Process 91
6.3.2.1 Pre-Selection 91
6.3.2.2 Relocation 91
6.3.2.3 Evaluation 92
6.3.2.4 Final Selection 93
6.4 Exploring the Mind of a Spy 93
6.4.1 Project Slammer 95

6.4.2 Personality Disorders 96
6.4.2.1 Antisocial Personality Disorder 96
6.4.2.2 Narcissistic Personality Disorder 97
6.4.3 Three Critical Factors and Traits Lead to Treasonous Betrayal 97
6.4.3.1 Character 98
6.4.3.2 Stress 98
6.4.3.3 Lack of Intervention 98
6.4.4 Positive Qualities Create a Strong Capacity for Loyalty 98
6.5 Categories of Spies 99
6.5.1 Government Spies 99
6.5.2 White-Collar Crime Not Involving Spies 100
6.5.3 Agents of Radicalization 101
6.6 Indicators of a Growing Problem 103
6.6.1 Government Spies 105
6.6.2 White-Collar Organized Crime Activity Spies 105
6.7 Concluding Remarks 105
Bibliography 107

CHAPTER 7 SPIES AND ESPIONAGE 109
7.1 Profile of a Spy 109
7.2 A Double Life 110
IBRAHIM I. CHALHOUB, PhD
7.3 Types of Spies 111
7.3.1 Local Spies 112
7.3.2 Internal Spies 112
7.3.3 Double Spies (aka "Double Agents") 113
7.3.4 Dead Spies 114
7.3.5 Living Spies 115

CHAPTER 8 SOCIAL ENGINEERING AND COUNTERMEASURES 117
8.1 Social Engineering 117
8.1.1 Social Engineering Defined 117
8.1.2 Who Uses Social Engineering 118
8.1.3 Social Engineering Techniques 119
8.1.3.1 Impersonation 119
8.1.3.2 Urgency 119
8.1.3.3 Name-Dropping 119
8.1.3.4 Pretending to Help 119
8.1.3.5 Persuasion or Intimidation 119
8.1.3.6 Friendliness 119
8.1.4 Four Phases of Social Engineering 120
8.1.4.1 Intelligence and Information Gathering 120
8.1.4.2 Gaining Trust 120

8.1.4.3 Exploiting Trust 121
8.1.4.4 Conducting and Action/Gaining Access 121
8.2 Countermeasures 121
8.2.1 Training and Awareness 122
8.2.2 Security Measures 122
Bibliography 123

Chapter 9 Deception Detection 125
9.1 Establish a Baseline 125
9.2 Common Suspicious Behaviors 125
9.2.1 Eye Contact 125
9.2.2 Change in Voice 126
9.2.3 Body Language 126
9.2.4 A Mixed Signal 127
9.3 Macro and Micro Expressions 127
9.3.1 Macro Expressions 128
9.3.2 Micro Expressions 129
9.4 Eye-Accessing Cues 129
9.5 Truth Detection Equipment 129
9.5.1 How Traditional Truth Detectors Work 129
9.5.2 1988 Employee Polygraph Protection Act (EPPA) 130
9.5.3 Legal Requirements 131
9.6 Your Intuition 131
9.7 Handwriting Analysis 131

Part III Personal Information Security

Chapter 10 Home Computer Security 135
10.1 E-Mail Issues 135
10.1.1 Passwords 135
10.1.2 Corresponding Online 136
10.1.3 Mail Bombs 137
10.2 Website/E-Commerce Issues 138
10.3 Social Networking and Cyberstalking 139
10.4 Other Issues 140
Bibliography 142

Chapter 11 Security while Traveling 143
11.1 Travel Preparations 143
11.2 Importance of Identification 144
11.3 Travel Precautions 145
11.3.1 Destination Arrival 145
11.3.2 Rental Vehicles 145
11.3.3 Hotel 145
11.3.4 Personal 146

11.4 Precautions while Staying in a Foreign Country 147
11.4.1 Protect Your Passport 147
11.4.2 Safeguard Your Laptop Computer 147
11.4.3 Establish Points of Contact 148
11.4.4 Keep a Low Profile 148
11.4.5 Shun Publicity 149
11.4.6 Local Laws 149
11.4.7 Money Matters 149
11.4.8 Medical Problems and Emergencies 150
11.4.9 Arrest 150
11.4.10 Illness or Medical Emergency 151

PART IV SECURITY WITHIN BUSINESSES

CHAPTER 12 SECURING BUSINESS SSI 155
12.1 Corporate Spying 155
12.1.1 Spy Techniques/Technology 155
12.1.2 Spy Techniques and Prevention 156
12.2 No Business Is Safe 157
12.3 International Organization for Standardization Guidelines 158
12.4 Choosing a Security Company 159
12.5 Responding to a Security Breach 160
12.5.1 Act Quickly 160
12.5.2 ISO 20002 Standards 160
12.5.3 Steps to Take 161
12.5.3.1 Assemble an Incident-Response Team 161
12.5.3.2 Assess the Initial Damage and the Risk for More 161
12.5.3.3 Develop a Notification Plan 162
12.5.3.4 Touch Nothing until a Forensics Team Is Called 162
12.5.3.5 Document Everything 162
12.5.4 Stopping the Next Attack 163
12.6 Preventing Physical Theft 163
12.7 Security Breach Notification Laws 164
12.7.1 Example of a Notification Law 165
12.7.2 Notification Process 165
12.7.2.1 California Office of Privacy Protection Recommendations 166
12.7.2.2 Model Letter 167
12.7.3 Federal Trade Commission (FTC) 167
12.8 Your Opportunity to Comment 168

CHAPTER 13 ANSI STANDARDS 169
13.1 The ANSI INCITS 359-2004 169
13.1.1 RBAC 169

13.2 ANSI INCITS 359-2004 Organization 170
13.2.1 Reference Model 170
13.2.2 Functional Specifications 170
13.2.2.1 Core RBAC 170
13.2.2.2 Hierarchical RBAC 170
13.2.2.3 Static Separation of Duty (SSD) Relations 171
13.2.2.4 Dynamic Separation of Duty (DSD) Relations 171
13.3 ANSI INCITS 359-2004 as the RBAC Standard 172
Bibliography 172

CHAPTER 14 CORPORATE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) 173
14.1 The Importance of Using the National Institute of Standards and Technology (NIST) 173
14.2 Due Care and Due Diligence 174
14.2.1 Due Care 174
14.2.2 Due Diligence 174
14.3 Processes and Methodologies 174
14.4 Advantages of Using NIST 175
14.4.1 Useful for Proving Due Care and Due Diligence 175
14.4.2 A More Thorough Approach 175
14.5 Conducting Risk Assessments 176
14.5.1 Perform Periodically 176
14.5.2 Maintain Records 176
14.5.3 Use an Outside Security Company 176
14.5.4 Use Continuously 177

CHAPTER 15 CYBERSECURITY 179
15.1 Information Storage and Transmission 179
15.1.1 Radicati Group 179
15.1.2 School of Information Management and Systems (SIMS) Study 179
15.1.3 Information Measurement Explained 180
15.2 Cybersecurity Challenges 180
15.2.1 Securing Large Amounts of Information in Various Locations 180
15.2.2 Securing All Workstations 181
15.2.3 Securing Electronic Forms of Communication 181
15.3 Protecting Your Most Sensitive Information 181
15.3.1 Maintaining Two Computer Systems 182
15.3.1.1 Benefits 182
15.3.1.2 Drawbacks 182
15.3.2 Minimum Precautions 183
15.4 E-Mail 183
15.4.1 Potential Dangers of E-Mail 184

15.4.2 Different Types of E-Mail 184
15.4.2.1 Company E-Mails 184
15.4.2.2 Monitored Company E-Mail 184
15.4.2.3 Outside E-Mail Accounts 185
15.4.3 The Dangers of Bypassing Official E-Mail Systems 185
15.4.3.1 White House Example 185
15.4.3.2 Unsecure Servers 185
15.4.3.3 Specific Problems 186
15.4.3.4 Emerging Technologies 187
15.5 Cyber Checklists 188
15.5.1 International Travel 188
15.5.2 Environment 188
15.5.3 Physical Security 188
15.5.4 System Security 189
15.5.5 Virus Protection 189
15.6 Data Storage Tips 190
15.6.1 Use Passwords Correctly 190
15.6.2 Store Data Separately 190
15.6.3 Encrypt Files 190
15.6.4 Virus Definitions 190
15.6.5 Firewalls 190
15.6.6 CDs and DVDs 191

PART V GOVERNMENT SECURITY NEEDS

CHAPTER 16 THE INTELLIGENCE PROCESS 195
16.1 Intelligence and Counterintelligence 195
16.1.1 Intelligence Defined 195
16.1.2 Intelligence versus Information 195
16.1.3 The Definition of Intelligence as a Process 196
16.1.3.1 Generating a Requirement 196
16.1.3.2 Collecting Information 196
16.1.3.3 Evaluating and Analyzing 196
16.1.3.4 Writing an Intelligence Report 197
16.1.3.5 Dissemination 197
16.1.4 Intelligence as a Discipline 197
16.2 Military Intelligence 198
16.2.1 CIA Defines Intelligence 198
16.2.2 Intelligence Subspecialties 199
16.2.3 Restrictions 200
16.2.3.1 Posse Comitatus Act 200
16.2.3.2 Executive Order 12333 200
16.2.4 Other Agencies 200
Bibliography 201

CHAPTER 17 THE LAW AND HOMELAND SECURITY 203
17.1 Background 203
17.2 Executive Summary 203
17.3 History of Electronic Surveillance and FISA Court 204
17.3.1 Electronic Surveillance and National Security 204
17.3.2 FISA 205
17.3.2.1 Warrants 205
17.3.2.2 Foreign Combatants 205
17.3.3 Foreign Intelligence Information (FII) 206
17.3.4 FISC 206
17.3.4.1 Court Proceedings 207
17.3.4.2 FISA Application 207
17.4 Political Fallout of Electronic Surveillance 207
17.5 Impact of Electronic Surveillance 208
17.5.1 Foreign Intelligence 208
17.5.2 Domestic Intelligence 209
17.5.3 Security Threats 209
17.5.4 NSA Monitoring 210
Bibliography 211

CHAPTER 18 THE DEPARTMENT OF HOMELAND SECURITY (DHS) STRUCTURE 213
18.1 Department Subcomponents and Agencies 213
18.2 Department Components 213
18.2.1 Directorate for National Protection and Programs 213
18.2.2 Directorate for Science and Technology 213
18.2.3 Directorate for Management 214
18.2.4 Office of Policy 214
18.2.5 Office of Health Affairs 214
18.2.6 Office of Intelligence and Analysis 214
18.2.7 Office of Operations Coordination 214
18.2.8 Federal Law Enforcement Training Center 214
18.2.9 Domestic Nuclear Detection Office 215
18.2.10 Transportation Security Administration 215
18.2.11 United States Customs and Border Protection 215
18.2.12 United States Citizenship and Immigration Services 215
18.2.13 United States Immigration and Customs Enforcement (ICE) 215
18.2.14 United States Coast Guard 215
18.2.15 Federal Emergency Management Agency 216
18.2.16 United States Secret Service 216
18.2.17 Office of the Secretary 216
18.2.18 Privacy Office 216
18.2.19 Office for Civil Rights and Civil Liberties 216
18.2.20 Office of Inspector General 217

18.2.21 Citizenship and Immigration Services Ombudsman 217
18.2.22 Office of Legislative Affairs 217
18.2.23 Homeland Security Advisory Council 217
18.2.24 National Infrastructure Advisory Council 218
18.2.25 Homeland Security Science and Technology Advisory Committee 218
18.2.26 Critical Infrastructure Partnership Advisory Council 218
18.2.27 Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities 218

PART VI LEGISLATION AND REGULATIONS

CHAPTER 19 GOVERNMENT LAWS 221
19.1 Economic Espionage Act of 1996 221
19.1.1 Defining *Trade Secret* 221
19.1.2 Two Provisions 222
19.1.2.1 Foreign Economic Espionage 222
19.1.2.2 Commercial Theft 222
19.1.3 Penalties 222
19.1.4 Protecting Trade Secrets 223
19.1.5 Limitations 224
19.1.6 Gillette® and Kodak® Cases 224
Bibliography 225

CHAPTER 20 GOVERNMENT AND HIPAA 227
20.1 SSI-Related Laws and Terminology 227
20.2 Access to Information 227
20.2.1 FOIA 228
20.2.2 The Privacy Act of 1974 228
20.2.3 The PATRIOT Act 228
20.3 Privacy of Electronic Data and Computers 229
20.3.1 Center for Democracy and Technology 229
20.3.2 Computer Crime and Intellectual Property Section (CCIPS) 230
20.3.3 Information Security and Privacy Advisory Board (ISPAB) 230
20.4 Cryptology 230
20.4.1 National Security Agency (NSA) 230
20.4.2 Computer Security Resource Center (CSRC) 231
20.4.3 Computer Professionals for Social Responsibility 231
20.4.4 Electronic Frontier Foundation (EFF) 231
20.4.5 Electronic Privacy Information Center (EPIC) 231

20.5 Privacy Laws 232
20.5.1 National Information Infrastructure Protection Act of 1996 232
20.5.2 Computer Security Act of 1987 232
20.6 Trade Secrets 232
20.6.1 Uniform Trade Secrets Act 233
20.6.2 Economic Espionage Act 233
20.6.3 Coca-Cola® Case 234

CHAPTER 21 NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) 235
21.1 NISP Overview 235
21.1.1 A Partnership 235
21.1.2 The Government–Industry Relationship 235
21.1.3 Purpose of the NISP 236
21.2 Classified Information 236
21.2.1 Classified 237
21.2.2 Secret 237
21.2.3 Top Secret 237
21.3 Components of the NISP (DOD) 238
21.3.1 User Agencies 238
21.3.2 Cleared Contractors 240
21.3.3 Defense Security Service 240
21.3.4 Facility Security Office Role 241
21.4 The FSO and the Industrial Security Representative (IS REP) 241
21.5 Structure of DSS: Industrial Security 242

CHAPTER 22 SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION CONTROL PROCEDURES 243
22.1 Policies to Control SBU Information 243
22.1.1 Introduction to the Term *SBU* 243
22.1.2 Computer Security Act Definition of *Sensitive* 243
22.1.3 SBU in Relation to the FOIA 245
22.1.4 Department of Justice Broadens Interpretation of Exemptions from FOIA 245
22.2 Policies to Protect Specific Types of Sensitive Information Involving Scientific and Technical Applications 247
22.2.1 Vulnerabilities 247
22.2.2 Critical Infrastructure Information Act of 2002 248
22.2.3 DOD and DHS Rules 248
22.2.4 Homeland Security Presidential Directive 7 248
22.2.5 Protected Infrastructure Information Program 249
22.3 SSI Controls: Transportation 249

22.4 Identifying and Handling SSI 251
22.4.1 Section 15.5 of Code of Federal Regulations (CFR) Title 49 251
22.4.2 "Need to Know" Specifics 252
22.4.3 The Marking of SSI 252
22.4.4 Federal Records Act 253
22.4.5 Critique of SSI Rules 254
22.5 Controls on Environmental Impact Information 255
22.5.1 Categorical Exclusions to FOIA 255
22.5.2 Exemptions 256
22.5.3 Critiques of Controls on Environmental Information 257
22.5.4 The Nuclear Regulatory Commission (NRC) Example 258
22.6 Controls on Unclassified Biological Research Information 259
22.6.1 Dual-Use Concerns 259
22.6.2 Governmental Control Proposals 260
22.6.3 National Science Advisory Board for Biosecurity 261
22.6.4 Views on Adequacy of Biosecurity Protection Policies 262
22.6.4.1 2006 National Academies Report 262
22.6.4.2 Inadequate Rules 263
22.6.4.3 Codes of Conduct/Self-Monitoring Policies 264
22.6.4.4 Peer Review 264
22.6.4.5 Risk Categories 265
22.6.4.6 Risk-Based Approach 265
22.6.4.7 Restrictions Frustrate Researchers 266
22.6.4.8 Ethics Education Option 266
22.6.4.9 UK Royal Society/Welcome Trust 2004 Paper 267
22.7 Issues Dealing with Geospatial Information 268
22.7.1 RAND Corporation's Three Filters 268
22.7.2 Homeland Security Guidelines 268
22.7.3 FOIA Exemption 269
22.7.4 National Geospatial Intelligence Agency (NGIA) Example 269
22.7.5 Expanding Use of Data 269
22.8 The DHS's SBU Directives 270
22.8.1 Controversy and Opposition 270
22.8.2 Types of Control Labels 270
22.8.3 Unclassified and Need to Know 271
22.8.4 Complete CRS Report 271

CHAPTER 23 OPERATION SECURITY: A LAW ENFORCEMENT CONCERN 273
23.1 The Role of Operational Security 273
23.2 Information Sources for Criminals 273
23.2.1 Press Releases/Media Stories 273
23.2.2 Agency Websites 274
23.2.3 E-Mails and Online Chat Rooms 274
23.2.4 Surveillance of Communications 274
23.2.5 Surveillance of Activities 274
23.2.6 Trash Receptacles 275
23.2.7 Sensitive Documents 275
23.3 Preventing Breach of Security 276
23.3.1 Countersurveillance 276
23.3.2 Do Not Discuss Sensitive Information 276
23.3.3 Secure Firearms and Weapons 276
23.3.4 Monitor Inmate Labor 277
23.3.5 Restrict Information Sharing with Other Agencies 277
23.3.6 Vigilant Background Checks for Clerical and Information Technology (IT) Personnel 277
23.3.7 Personal Security 278
23.4 Developing a Security Plan 278

CHAPTER 24 CAMERA SURVEILLANCE 279
DENNIS TREECE
24.1 Setting up Camera Surveillance 279
24.1.1 Step One: Decide on Purpose 279
24.1.1.1 Prevention 279
24.1.1.2 Capturing Images for Later Use 279
24.1.1.3 Combination Approach 280
24.1.2 Step Two: Assess Existing Technology 280
24.1.3 Step Three: Decide Details 280
24.1.3.1 Frame Rate 280
24.1.3.2 Resolution 281
24.1.3.3 Compression 281
24.1.3.4 Storage Duration 281
24.1.3.5 Storage Size 281
24.1.3.6 Digital versus Analog 282
24.1.3.7 Pan Tilt Zoom (PTZ) 282
24.2 Issues to Consider 282
24.2.1 Monitoring 282
24.2.2 Decoys 283
24.2.3 Staffing 283
24.2.4 Privacy 283
24.2.5 Signage 283

24.2.6 Policies and Procedures 284
24.2.7 Training 284
24.2.8 Maintenance 284

CHAPTER 25 EAVESDROPPING THREATS AND IP PHONE SYSTEMS 285
25.1 Eavesdropping Threats 285
25.1.1 Influences on Eavesdropping 285
25.1.2 Evaluating the Threat 285
25.2 IP Phone Systems 287
RAINER A. MELUCCI, CSC, CFC, DABFE, CHS-III P.I.
25.2.1 Explanation of IP 287
25.2.2 Threats Associated with IP Systems 287
25.2.2.1 Remote Access 287
25.2.2.2 Packet Sniffing 287
25.2.3 Security Measures 288
25.2.4 NIST Recommendations 288

CHAPTER 26 FACILITY SECURITY 295
26.1 Homeland Security Presidential Directive 12 295
26.2 Who Manages the PIV Program? 296
26.3 What Do You Need to Implement PIV-I? 297
26.4 What Do You Need to Prepare for PIV-II? 299
26.5 Integration with Existing Infrastructure 299

PART VII IDENTITY THEFT

CHAPTER 27 FAIR AND ACCURATE CREDIT TRANSACTIONS ACT 305
27.1 Overview 305
27.2 What Is FACTA? 305
27.2.1 Section 114 (Special Rules for Card Issuers) 306
27.2.2 Section 315 (Address Discrepancy Rules) 306
27.3 What Agencies Promulgated the Red Flags Rule? 306
27.4 FACTA Guidance 307
27.4.1 Financial Institutions 307
27.4.2 Creditors 307
27.4.3 Covered Accounts 308
27.4.4 Transaction Accounts 308
27.5 Penalties for Non-Compliance to Red Flags 308
27.5.1 Federal 308
27.5.2 State 308
27.5.3 Civil 309
27.6 Benefits of Complying to Red Flags 309

CHAPTER 28 IDENTITY THEFT RED FLAGS UNDER FACTA 311
28.1 Red Flags 311
28.1.1 Definition 311
28.1.2 Examples of Red Flags 311
28.2 Identity Theft Defined 315
28.3 Types of Identity Theft 316
28.3.1 Four Main Risk Areas 316
28.3.2 Personal Identifiable Information (PII) 316

CHAPTER 29 DEVELOPMENT AND IMPLEMENTATION OF A RED FLAGS PREVENTION PROGRAM 317
29.1 Written Program 317
29.1.1 Charter 317
29.1.2 Risk Assessment 318
29.1.2.1 Identify Overseer 318
29.1.2.2 Collect Information 318
29.1.2.3 Establish a Risk Assessment Team 319
29.1.2.4 Identify Risk Assessment Methodology 319
29.1.2.5 Conduct the Risk Assessment 320
29.1.2.6 Identify Theft Risk to Data 321
29.2 Administering the Program 321
29.2.1 Identifying Relevant Red Flags 322
29.2.2 Detecting Red Flags 322
29.2.3 Responding to Red Flags 323
29.2.4 Preventing and Mitigating Identity Theft 323
29.2.5 Updating the Program 324
29.2.6 Establishing an Identity Theft Training Program 324
29.2.7 Oversight of Service Provider Arrangements 325
29.2.8 Obtaining Approval of the Initial Written Program by the Board of Directors 325
29.2.9 Address Discrepancy Rules 326
29.2.9.1 Comparing Information 326
29.2.9.2 Develop Reasonable Policies and Procedures 326
29.2.9.3 Confirm the Address 326
29.2.10 Special Rules for Card Issuers 327
29.3 Maintaining an Identity Theft Red Flags Program 327
Bibliography 328

PART I
Perspective

CHAPTER 1 The History of SSI
CHAPTER 2 Terms and Definitions
CHAPTER 3 The Importance of SSI
CHAPTER 4 The History of the SSI Classification System

1
The History of SSI

1.1 The Context of Sensitive Security Information (SSI)

1.1.1 First Use of the Term SSI

The term *sensitive security information* first appeared in 1974, when the Federal Aviation Administration (FAA) tried to anticipate airplane hijackings by collecting information from airlines, sometimes personal, about passengers. The FAA withheld this information from the public. During this time, SSI was limited to information concerning the safety of passengers. The FAA's definition and use of SSI withstood testing in 1993, when a Washington, DC, court ruled that SSI did not fall under the authority of the Freedom of Information Act.

1.1.2 Effects of 9/11

Immediately after the terrorist attacks of September 11, 2001, national security became the most important concern for the United States. Regulations relating specifically to transportation increased, because the attacks involved the hijacking of commercial airline planes. Congress passed legislation that created the Transportation Security Administration (TSA), a division of the Department of Homeland Security. Part of the responsibility of the TSA was to develop regulations for SSI. Because Congress passed this legislation after September 11, 2001, SSI has fueled a debate about when information should be shared with the public and when it should be kept secret.

Within 2 months of the September 11 attacks, Congress passed the Aviation and Transportation Security Act, which allowed it to pass a bill creating the TSA as an agency of the Department of Homeland Security. Then Congress passed the Homeland Security Act. These pieces of legislation contained tiny changes that

translated to a big expansion in the meaning of SSI. In the bill creating the TSA, the word *air* was dropped before *passengers*, which had the effect of extending SSI to all types of passengers. Next, the Homeland Security Act also omitted *passengers*, which meant that more information would fit into the definition of SSI, not just information about passengers.

1.2 Defining SSI

1.2.1 Early Definitions

The definition of SSI has greatly expanded in the wake of September 11, 2001. Once, SSI had applied only to airline passengers, but the new definition includes other types of travel and, according to the Coalition of Journalists for Open Government, any information that the TSA, Coast Guard, or Department of Transportation finds could be dangerous to the security of transportation if disclosed. The information needs only a connection to transportation of any sort, even including pipelines. Authority rests with the TSA administrator to decide whether disclosure would put passenger safety at risk. If information receives the SSI designation, then disclosure occurs on a need-to-know basis, which the TSA determines.

1.2.2 Current Definition

The TSA now defines SSI as "unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of federal operations or assets, the health and safety of the public, or the nation's long-term economic prosperity." If the TSA considers information to be SSI, then that information may be kept from the public.

One important point to remember with the government's definition of SSI is that only information regarding transportation security and not other types of security may be classified as SSI. Also, SSI may be kept private solely on the discretion of the TSA and not for specific or limited reasons. No time limits for release of information or declassification of SSI exist. All of these factors contribute to the controversy that the TSA has too much power.

1.2.3 Designating SSI

SSI needs to be protected to prevent its disclosure. If a document contains SSI, then that document must have a protective marking and a statement clearly stating the existence of SSI in its content.

The United States Code contains the Aviation and Transportation Security Act, including provisions for SSI, in Title 49. Relevant sections are 114(s) and 40119. The TSA has regulations called Transportation Security Regulations that address administrative, procedural, and security issues for transportation. Part 1520 of Subchapter A of the regulations pertains to SSI, and the Code of Federal Regulations contains this information in 49 C.F.R. § 1520.

An article from the Congressional Research Service, "Sensitive Security Information and Transportation Security: Issues and Congressional Options," by Mitchel A. Sollenberger (2004), presents steps the government could take to balance national security with the public's right to know. The article points out that the existing regulations and laws could simply remain as they are. A second option would be for Congress not to allow the TSA to have such sweeping power but to require more specificity in the regulations. Still another option would be for Congress to create an advisory committee to analyze SSI and suggest improvements or alternatives. One of the other options mentioned in the article would be to create an entity to oversee TSA's use and management of SSI.

One recent case involving the disclosure of SSI involves the firing of a federal air marshal for sharing information about the TSA's unclassified plan to remove air marshals from nonstop long-distance flights. Federal Air Marshall Robert MacLean filed documents with the Ninth Circuit Court of Appeals to oppose the TSA's claim that the plan is SSI. He went public with some sensitive information because of his conviction that the TSA was allowing a loophole that could allow terrorists to get their operatives on flights to the United States by checking in countries that have lax security procedures. MacLean is the first person to be fired for releasing SSI (Losey, 2006). How the court interprets the power of the TSA could set important precedent for future cases.

With SSI being a relatively new classification and with the security of information still an important issue, modifications to its scope or

definition will probably occur. The SSI issue is still evolving and care should be taken to maintain current information about changes to the definition.

1.3 Securing SSI

In a world of ever-changing technology, with massive amounts of information available to the public in a matter of seconds, secure information is at risk of being exposed to unauthorized viewers. Government, businesses, and individuals must take extra precautions in securing their SSI. SSI is important in security of all types including company, transportation, and government.

Spies have been a threat to sensitive information since the beginning of time. To best protect from the threat of spies, groups should understand the different techniques, known patterns, types, and case studies of spies. Individuals should also protect their SSI by staying current with security measures for their personal computers and protecting SSI documents while traveling. Other security measures for securing sensitive information involve camera surveillance, securing phone systems, and perform physical/facility security enhancements.

Following proper measures aids in the protection of the sensitive information, although it does not ensure it. A person's, company's, or government's best defense against an SSI breach is to stay informed on current security measures and pursue them.

Bibliography

Classified information. (2006). *Wikipedia*. Retrieved June 26, 2006, from http://en.wikipedia.org/wiki/Classified_information.

Harshaw, K.G. & McKerral, G. (2004, June 16). Roadblock: In the name of security, government shields access to transportation. Retrieved January 29, 2007, from http://www.asne.org/index.cfm?ID=5251.

Losey, S. (2006). Air marshal's firing prompts whistleblower suit. Retrieved August 9, 2007, from FederalTimes.com website: http://www.federal-times.com/index.php?S=2331806.

National Security Briefing. (n.d.). Retrieved July 26, 2006, from http://www.wasc.noaa.gov/wrso/brefings/nsb.pdf.

NetLaw. (2001, May 8). Confidential information. Retrieved July 11, 2006, from http://www.oznetlaw.net.

Pike, J. (2002). Security and classification. Retrieved June 27, 2006, from http://www.tscm.com/classification.html.

PR Newswire. (2006, October 30). Department of homeland security violates whistleblower Protection laws. Retrieved January 28, 2007, from http://news.findlaw.com/prnewswire/20061030/30oct20061256.html.

Sensitive Security Information. (n.d.). Retrieved January 27, 2006, from http://www.dss.mil/training/csg/security/S2unclas/Ssi.htm.

Smart Agreements.com. (2005). Confidential information. Retrieved July 11, 2006, from http://www.smartagreements.com/biotopics/Bltopic2.html.

Sollenberger, M.A. (2004, June 9). Sensitive security information and transportation security: Issues and congressional options. Retrieved January 29, 2007, from http://www.fas.org/sgp/crs/RL32425.pdf.

The Economic Espionage Act of 1996. (1996). 18 U.S.C. §§ 1831–1839.

Unocal. (2003, March). Unocal code of conduct: Business ethics. Retrieved June 26, 2006, from http//www.unocal.com/ucl_code_of_conduct/ethics/information.html.

Weitzel, P. (2004, November–December). Beware regulatory creep as secrecy shrouds records. FOI Columns. Retrieved January 29, 2007, from http://www.ire.org/foi/novdec2004.html.

2
Terms and Definitions

SSI is relevant in three distinct areas:

- Government (National Security and Safety);
- Public (Asset Protection of the Company); and
- Private (Personal Identity and Credit Worthiness).

2.1 Government Information

The government is the most important area of secrecy, as government secrets affect the majority of individuals in the country and are vital for keeping our nation safe and for ensuring our freedoms. Secret information on the national level is most often referred to as *classified* (that owned and or under the control of the United States government and that certain classes of individuals are restricted from accessing by law or regulation). The classification system is designed to protect the confidentiality of the national defense and foreign relations of the United States. Classified information in the United States falls under one of three categories: confidential classification, secret classification, and top secret.

2.1.1 Confidential Classification

Confidential classification relates to information or material that, if disclosed without proper authorization, would cause damage to our national security (such as the compromise of the strength of ground, air, and naval forces in the United States and overseas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; or revelation of performance characteristics, test data, design, and production data on munitions of war).

2.1.1.1 Sensitive Security Information (SSI) Recap After the terrorist attacks of September 11, 2001, Congress created the TSA to safeguard the nation's transportation system. Among its duties, the TSA was empowered to designate and protect sensitive security information. The information to be restricted included plans for security and details about our transportation system that could prove useful to terrorists. Since that time, private sector information specialists have loosely borrowed the term to define information essential to the security of businesses, including vital trade secrets. This guide employs both uses of the phrase.

2.1.2 Secret Classification

Secret classification pertains to information or material that, if disclosed without proper authorization, would cause serious damage to national security (such as the disruption of foreign relations, the compromise of significant scientific or technological development, and the impairment of a program or policy).

2.1.3 Top Secret

Top secret, the highest level of classification, encompasses intelligence that, if disclosed without proper authorization, would pose a great threat of unparalleled and extensive damage and/or harm to our nation's national security (such as armed hostilities toward the United States, the disruption of foreign relations, and the compromise of vital national defense plans).

2.2 Public Information

Public information is generally referred to as confidential information and usually pertains to any information relating to a company's business that the company develops, discovers, or obtains. This information is kept private and, if improperly disclosed, could cause damage to the company. Confidential information, which varies widely in terms of complexity and value, includes but is not limited to the following areas:

- Software programs
- Computer passwords
- Business plans
- Processes
- Marketing plans
- Product formulations
- Financial statements
- Operations information
- Customer lists
- Trade secrets

2.2.1 Trade Secrets

The most common type of confidential information is a trade secret. Although the terms *confidential information* and *trade secre*t are often used interchangeably, a trade secret is actually one of many subsets of confidential information.

The Economic Information & Trade Secrets Act of 1996 defines trade secrets as

> all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:
> The owner thereof has taken reasonable measures to keep such information secret, and; the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.

Simply stated, in order for information to be considered a trade secret, it must have an economic value, must not be common knowledge to the majority of the population, and must not be information that could be discovered by other parties through proper means due to the efforts put in place by the owner to keep the information confidential. Maintaining the secrecy of confidential information such

as trade secrets is important so that businesses can have an advantage over their competitors and, as a result, enjoy higher profits.

2.2.2 Information Theft

Information theft is easy, safe, and lucrative. Eavesdropping laws are difficult to enforce. Advancements in electronics and optoelectronics have made communications interception easy and inexpensive. Competition is now global. There are more competitors than ever before.

Some of the tactics information thieves use to accomplish their goals include tapping phones, bugging offices, stealing papers, covert recordings, undercover employees (moles), phony repair people, car phone monitors, fax intercepts, pretext calls, dumpster divers, competitive intelligence professionals, renegade employees, and foreign governments.

2.3 Personal Information

Personal information is any information that can identify an individual, including but not limited to

- Social Security numbers
- Driver's license numbers
- Names
- Mailing addresses
- E-mail addresses
- Bank account numbers
- Credit card numbers
- Phone numbers
- Health information
- Ages

2.3.1 Responsibility of Secrecy

Maintaining the secrecy of personal information is the responsibility of the individual, the individual's employer, and any other institution, company, or business to which an individual has disclosed his or her personal information under terms guaranteeing the confidentiality of

the personal information disclosed. The confidentiality of personal information is important to ensure the physical safety of individuals, to prevent identity theft, and to protect individuals' rights to privacy.

2.3.2 Breaches in Personal Information

If a person's financial information has been breached, it is recommended that they *not* be notified via e-mail. Consumers/customers should be contacted if their sensitive personal information is breached, such as Social Security numbers and banking information. They need to be informed so they can take action to monitor their financial information. Thirty-six states have mandatory information breach laws.

2.4 Sensitive but Unclassified (SBU) Information

SBU information should be protected as well as the information mentioned above. The term was first used in the 1970s but has never been defined in statutory law.

2.4.1 SSI Designation

As spelled out in 49 CFR § 1520.7, SSI is a control designation used by the Department of Homeland Security, and particularly the TSA. It is applied to information about security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation.

However, in this book of knowledge, we broaden the definition of SSI to any information that is sensitive to our nation's security. SSI can also relate to sensitive corporate information and even personal information. SSI applies to information that the government obtains from the private sector or develops on its own while carrying out certain security or research and development activities. It protects information that, if disclosed, would be an unwarranted invasion of personal privacy, reveal a trade secret or privileged or confidential commercial or financial information, or make it easier for hostile elements to avoid security controls.

2.4.2 SBU Designations

Federal agencies report using 56 different SBU designations to protect sensitive information—from law or drug enforcement information to controlled nuclear information—and agencies that account for a large percentage of the homeland security budget report using most of these designations. These designations include the following:

1. Applied Technology: Department of Energy (DOE)
2. Attorney–Client Privilege: Department of Commerce (Commerce), DOE
3. Business Confidential: DOE
4. Budgetary Information: Environmental Protection Agency (EPA)
5. Commerce
6. Confidential Information Protection and Statistical Efficiency Act Information (CIPSEA): Social Security Administration (SSA)
7. Computer Security Act Sensitive Information (CSASI): Department of Health and Human Services (HHS)
8. Confidential: Department of Labor
9. Confidential Business Information (CBI): Commerce, EPA
10. Contractor Access Restricted Information (CARI): HHS
11. Copyrighted Information: DOE
12. Critical Energy Infrastructure Information (CEII): Federal Energy Regulatory Commission (FERC)
13. Critical Infrastructure Information: Office of Personnel Management (OPM)
14. Drug Enforcement Administration (DEA) Sensitive: Department of Justice (DOJ)
15. Department of Defense (DOD) Unclassified Controlled Nuclear Information: DOD
16. Draft: EPA
17. Export Controlled Information: DOE
18. For Official Use Only (FOUO): Commerce, DOD, Department of Education, EPA, General Services Administration, HHS, DHS, Department of Housing and Urban Development (HUD), DOJ, Labor, OPM, SSA, Department of Transportation (DOT)

19. For Official Use Only, Law Enforcement Sensitive: DOD
20. Freedom of Information Act (FOIA): EPA
21. Government Confidential Commercial Information: DOE
22. High-Temperature Superconductivity Pilot Center Information: DOE
23. In Confidence: DOE
24. Intellectual Property: DOE
25. Law Enforcement Sensitive: Commerce, EPA, DHS, DOJ, HHS, Labor, OPM
26. Law Enforcement Sensitive/Sensitive: DOJ
27. Limited Distribution Information: DOD
28. Limited Official Use (LOU): DHS, DOJ, Department of Treasury
29. Medical Records: EPA
30. Non-Public Information: FERC
31. Not Available: National Technical Information Service, Commerce
32. Official Use Only (OUO): DOE, SSA, Treasury
33. Operations Security Protected Information (OSPI): HHS
34. Patent Sensitive Information: DOE
35. Pre-decisional Draft: DOE
36. Privacy Act Information: DOE, EPA
37. Privacy Act Protected Information (PAPI): HHS
38. Proprietary Information: DOE, DOJ
39. Protected Battery Information: DOE
40. Protected Critical Infrastructure Information (PCII): DHS
41. Safeguards Information: Nuclear Regulatory Commission (NRC)
42. Select Agent Sensitive Information (SASI): HHS
43. Sensitive but Unclassified: Commerce, HHS, National Aeronautics and Space Administration (NASA), National Science Foundation (NSF), Department of State, U.S. Agency for International Development (USAID)
44. Sensitive Drinking Water Related Information (SDWRI): EPA
45. Sensitive Information: DOD, U.S. Postal Service (USPS)
46. Sensitive Instruction: SSA
47. Sensitive Internal Use: DOE

48. Sensitive Unclassified Non-Safeguards Information: NRC
49. Sensitive Nuclear Technology: DOE
50. Sensitive Security Information (SSI): DHS, DOT, U.S. Department of Agriculture (USDA)
51. Sensitive Water Vulnerability Assessment Information: EPA
52. Small Business Innovative Research Information: DOE
53. Technical Information: DOD
54. Trade Sensitive Information: Commerce
55. Unclassified Controlled Nuclear Information (UCNI): DOE
56. Unclassified National Security-Related: DOE

Bibliography

http://www.schneier.com/blog/archives/2006/05/us_government_s.html.

3
The Importance of SSI

3.1 Dangers to Sensitive Information

"Guard against trust and complacency." Heed that admonition, and you are well on your way to becoming a successful SSI professional. You must cultivate a healthy distrust, especially of your skills as a judge of character. Realize that the work you do to protect sensitive information will never be complete, and your opponents will never stop thinking of new ways to overcome your defenses.

3.1.1 Trust

Trust is a good thing. As a child, you trust your parents, and for the great majority of us that trust is well placed. In faith, most put their trust in God, and although they do not always understand why some things happen, they have faith that they will never be abandoned. There are still a (very) few things in life where you know your trust will never be violated.

Most of the time, however, complete trust is foolish. Everyone has experienced the disappointment of a misplaced confidence. Few feelings are worse than those that broken trust provokes, and the damage done can range anywhere from hurt feelings to financial loss, a broken marriage, a ruined business—and perhaps much worse. If you work in a profession that handles SSI, either under the strict government definition or the popular private sector usage, your tendency to trust people you think you know can lead you and your organization into deep trouble.

Looking back at the history of humankind, we see over and over that there cannot be a betrayal without trust first. The betrayed almost always believed in their instincts, their gut feelings, and they knew

that the person or people they invested their trust in would never let them down. Only after the broken trust did they realize that they had also been betrayed by their own judgment. They were not the expert judges of character that they had imagined themselves to be. No one is—not one person.

Think of the greatest national security breach our nation has experienced—the treason committed by the highly placed Federal Bureau of Investigation (FBI) agent Robert Hanssen, who swore to defend our nation from its adversaries. Then, over a course of 15 years, he sold America's most sensitive secrets to the Soviet Union. The United States suffered staggering blows to its security, and brave men who supported us in Russia were brutally executed because Hanssen traded his loyalty for money. There are many other instances of espionage, deception, and thefts great and small. Many will remember the matter of Sandy Berger, the National Security Advisor during the Clinton administration, who was caught in 2004 stealing classified documents relating to events leading up to the terrorist attacks of September 11, 2001. Berger had convinced a National Archives executive to let him examine classified documents without going through the proper procedure of reviewing the information under close supervision in a secure room. After all, he was an important person, was he not? He was the former National Security Advisor. He was someone who could be trusted.

As it turned out, he was guilty, at the very least, of taking highly sensitive documents from the National Archives. His detractors say that he stole and destroyed documents that would have put the Clinton administration's efforts to head off terrorism in a bad light. In either case, his case serves as a warning that security procedures must be applied to the letter in all cases, no matter who is involved.

3.1.2 Complacency

In recent times, the business world has been rocked by high-profile thefts of information. Some of the cases involved the theft of personal data from hundreds of thousands of customers who are now at higher risk of identity theft. In those cases, the problem was not that companies had too much trust—it was that they did not have the procedures in place to prevent the thefts. All too often, the thefts happened

because those who handle the sensitive information did not have the foresight and the ability to think creatively about the threats that existed and how to thwart them before espionage could take place. They had a false sense of security; they were complacent.

Thefts also happened because established procedures were either unknown or not followed to the letter. Many corporations in America continue to be vulnerable because they have chosen efficiency over security. For instance, open access to computers often promotes productivity—that is, until an employee brings in a virus on a flash drive or by e-mail accidentally copies sensitive information to the wrong person.

Each year, American businesses lose billions of dollars because of corporate espionage, both foreign and domestic. In a 2005 report to Congress on Foreign Economic Collection and Industrial Espionage, the Office of the National Counterintelligence Executive stated that 108 nations were suspected of being involved in espionage against American businesses. The financial losses are untold, because much of the espionage either went unnoticed or was not reported because businesses did not want adverse publicity. Conservative estimates place the annual financial damage at around $60 billion, including the loss of thousands of American jobs.

3.1.3 Espionage

It is impossible for one resource to provide a set list of procedures that will be 100 percent effective in preventing compromises of sensitive information. This book will give those responsible for dealing with sensitive information the tools they need to understand security threats and the insight to be able to stay one step ahead of the cunning 21st-century thieves, spies, and traitors.

A survey of 1000 U.S. companies conducted in 1999 for the American Society for Industrial Security reported that 579 of them suffered losses of proprietary information. The estimated loss of intellectual property was $45 billion. Just 2 years later, the 2001 estimate was $59 billion, with an average of 2.45 incidents reported per company. Manufacturers in the survey reported fewer incidents, but their average loss per incident was estimated at nearly $50 million. The 1999 Annual Report to Congress on Foreign Economic Collection

and Industrial Espionage estimated that the actual amount lost to espionage may have been $300 billion—and by all accounts, the problem has worsened since then.

The damage done to American businesses through trade secret theft and economic espionage is staggering. It is growing as more information goes online, and as employees have fewer and fewer qualms about job-hopping and sharing information about their previous employers. Globalization is forging many alliances among international investors and United States companies, and as more foreign nationals enter the picture, the chances for trade secret theft will only multiply.

Although lines continue to blur as American companies invest globally and global companies invest in and acquire U.S. companies, corporate espionage can still be broken down into two categories: foreign and domestic.

Espionage from foreign sources usually comes from one of two sources—rival foreign businesses and manufacturers and foreign government entities, including intelligence agencies and services.

Privately held businesses may receive assistance from their governments to carry out espionage in America. U.S. intelligence reports often state that China and Russia by far account for the most cases of espionage against U.S. companies.

By far, the costliest forms of computer attack during 2004, as reported in a 2005 survey, were viruses, unauthorized access, and thefts of proprietary information (Figure 3.1).

According to the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2005, foreign espionage collectors were observed

- Exploiting U.S. business for technology to strengthen the capabilities of their nation
- Positioning their people at U.S. military bases to learn classified information in order to improve their military modernization efforts
- Hiring U.S. commercial firms to identify and acquire U.S. technology
- Going to U.S. academic institutions to recruit students, professors, scientists, and researchers to engage in technology collection

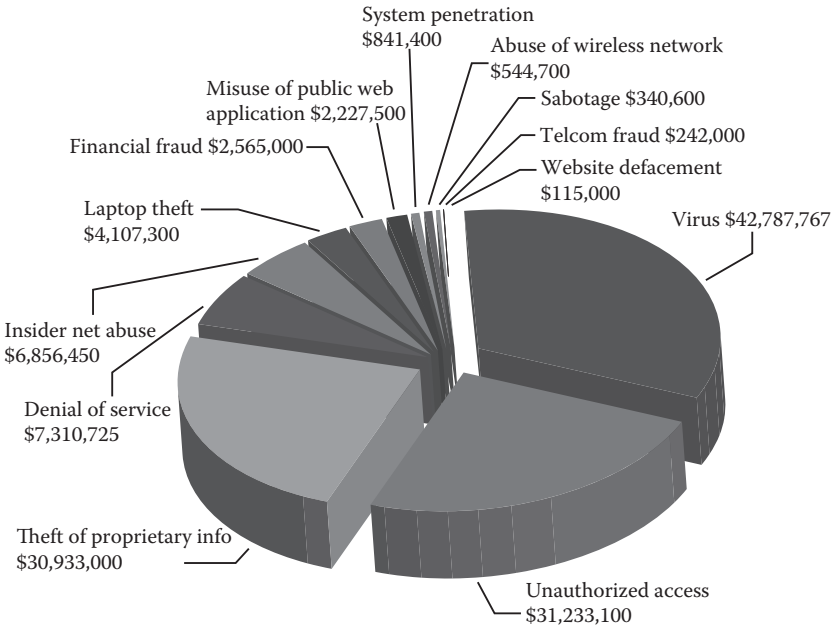

Figure 3.1 Computer attack losses by type.

The report states that corporate espionage collectors relied mainly on the least expensive, easiest, and safest methods available to them to harvest corporate information. Their techniques listed below were basic:

- **Asking**—The information seekers simply made direct requests for classified, sensitive, or export-controlled information. A single buyer can send requests to many U.S. companies at once, and then they can take advantage of any company that is willing to make a profit by bending or ignoring export-licensing requirements.
- **Ventures**—Companies can form ventures with U.S. businesses with the hope of placing their agents in close contact with sensitive technologies.
- **Services**—Foreign companies offer technical services to U.S. research facilities or cleared defense contractors. Then they try to glean as much information as they can about protected technologies.
- **Visitors**—Foreign governments and businesses will send their people to visit the United States and collect information at conventions and expositions.

- **Online**—Companies and governments use their technology experts to harvest information on password-protected Internet sites or through other online avenues.

3.2 Thwarting Economic Espionage

Billions of U.S. dollars are lost to foreign competitors who target economic intelligence in flourishing U.S. industries and technologies, and who cull intelligence out of shelved technologies by exploiting open source and classified information known as trade secrets.

The FBI is proactive in its approach to economic espionage. It is the FBI's number two priority, second only to terrorism. The FBI's Economic Espionage Unit is dedicated to countering the economic espionage threat to include developing training and outreach materials; participating in conferences; visiting private industry; working with the law enforcement and intelligence community on requirement issues; and providing specific classified and unclassified presentations.

3.2.1 Creating Spy Networks

Foreign competitors who criminally seek economic intelligence generally operate in three ways to create their spy networks:

- They aggressively target and recruit susceptible people (often from the same national background) working for U.S. companies and research institutions.
- They recruit people to find economic intelligence through operations such as bribery, discreet theft, dumpster diving (in search of discarded trade secrets), and wiretapping.
- They establish seemingly innocent business relationships between foreign companies and U.S. industries to gather economic intelligence, including classified information.

3.2.2 Acquiring Trade Secrets

Methods used to acquire trade secrets include

- Stealing, concealing, or carrying away by fraud, artifice, or deception

- Copying, duplicating, sketching, drawing, taking a photograph, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying
- Receiving, buying, or possessing a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization

3.2.3 Protecting against Espionage

Six steps can be taken to protect your business from espionage and they are as follows:

- Recognize that there is a real threat.
- Identify and evaluate trade secrets.
- Implement a definable plan for safeguarding trade secrets.
- Secure physical trade secrets and limit access to trade secrets.
- Confine intellectual knowledge.
- Provide ongoing security training to employees.

3.3 Sensitive Information and Where It Exists

3.3.1 Types of Sensitive Information

A white paper published in 2003 by Xerox, "Economic Espionage and Trade Secret Theft: Defending against the Pickpockets of the New Millennium," outlines the most sought-after information that corporate espionage seeks. The list below identifies types of information protected as trade secrets and prosecuted under the Economic Espionage Act of 1996:

- Access card control information
- Project information
- Pricing information/sales forecasts
- Financial information
- Computer source code
- Test material/prototypes/design specifications
- Customer business information
- Engineering plans and drawings

- Formulas
- Research
- Blueprints/diagrams
- Confidential documents
- Software
- Implementation methodology
- Technical records
- Biomedical research
- Sales forecasts

3.3.2 Sensitive Information Locations

This information exists in countless locations within an organization. One of the first tasks a new information security professional should undertake is to perform an analysis to identify SSI in all its forms and to establish categories that rank the information according to its sensitivity. It is not a task that should be rushed, as it requires conversations with employees at all levels of an organization to understand the information at their disposal and how they access it, process it, store it, and send it. The information security professional should think creatively about this information. He or she should use deductive reasoning to project what vulnerabilities may exist as the information progresses through planning, creation, temporary storage, implementation, publication or transmission if applicable, and ultimate storage or destruction. It is often helpful to create a flow chart that maps the stages that a project or data file goes through within the organization. At each level, draw arrows and label the people who may have access to the information. This is known as establishing the chain of custody. Again, think creatively and do not limit your deductions. For instance, information left on a dry erasure board in a conference room may be accessible by anyone who subsequently uses the room, including the janitor who cleans it. Notes that are taken may be discarded in a waste receptacle, where they can be accessed by people engaging in corporate espionage either inside or outside an organization.

Use the information presented in this guide as a starting point. Keep in mind that every government agency or business is unique and has its own security needs. It is up to you, through a process

of conversations, analysis, and forward reasoning, to plot out where vulnerabilities exist, who may seek to exploit them, and how they may conduct an attack.

Read lists other security professionals have created. The field of information security is often open, and security professionals are willing to share some of their expertise in order to help fellow professionals, as long as they do not divulge information that might affect their own security efforts. For instance, the Xerox white paper already cited also identifies areas where the trade secrets of a government agency or private company often reside:

- Computer files
- Formal or draft documents
- Working papers (including notes and action lists)
- Scrap papers
- Appointment calendars
- Internal correspondence
- Newsletters
- Policy documents
- Meeting minutes
- Legal and regulatory filings
- Annual reports
- Patent applications
- Travel documents
- Other official records
- Trash receptacles inside a building or trash bins on the outside
- The memories of employees

3.3.3 Overlooked Sources of Sensitive Information

There are many forms of computer files that are not in the form of a readily recognizable word processing, spreadsheet, design template, or e-mail file. As further food for thought, here are some of our recommendations for the not-so-obvious sources of sensitive electronic information:

1. Internet Cookies

   These are hidden files that store information from websites, such as user names and passwords.

2. Internet Caches

   Web pages that have been loaded previously are saved so that the Internet browser can more quickly load pages with elements that have not changed.

3. Browser-Based Web Histories

   Browsers can store records of all web pages visited, and the user has the option of setting how long the histories go back.

4. Download Histories

   Web browsers record what files have been downloaded, where they came from, and the location from where they were initially downloaded.

5. Search Engine Histories

   Companies such as Google offer a service that allows users to search the history of their own searches, which adds the convenience of being able to find the results of earlier searches. The downside, of course, is that through hacking or password theft, an outsider would have the same easy access to this highly sensitive information.

6. Third-Party E-mail Accounts

   An employee may set an e-mail preference that automatically forwards to an outside account. This may be done innocently for convenience to work from home, or so that an employee will have the information in case of future litigation (wrongful termination). Or it can be done as part of corporate espionage (corporate mole).

7. Information Technology (IT) Department Records

   IT professionals have the ability to keep detailed records of every site visited by an organization's employees. They can also track, store, and access any incoming or outgoing e-mail. A corporate espionage collector in the IT department could have more access to sensitive information than even the top-level executives of a company or government agency. Even if there is no mole in IT, the information rests on the IT computers and could possibly be accessed by a tech-savvy insider or possibly even a resourceful outside computer hacker.

3.4 Identifying Computer Vulnerabilities

Your company's IT professionals will be your best resource for identifying computer vulnerabilities and taking action to eliminate them. Web usage reports kept by the IT department can identify website and e-mail patterns and determine whether any suspicious activity should be investigated. Firewalls can be adjusted to block certain sites from being visited or to prevent outgoing messages from being delivered to certain destinations (such as an employee's Gmail account).

Some IT professionals may be overconfident in the security system they have established, and they may react defensively to an information security inquiry. The information security professional should emphasize that no single person, not even a department, can identify all forms of present or future risk. Information security is a collaborative process, and the information security professional must work closely with IT to provide maximum security for sensitive information. The information security professional must also have enough information about computer systems and vulnerabilities to be able to ask good questions of IT and raise valid concerns. This guide will provide a good foundation from which to start.

3.5 Domestic Economic Espionage

Rival businesses and manufacturers within the United States also conduct corporate espionage using both legal and illegal means. In fact, espionage or information collecting is so widespread that an organization has formed to serve professionals who legally and ethically gather business intelligence. The Society of Competitive Intelligence Professionals (http://www.scip.org) formed in 1986 and today has more than 50 chapters around the world, with members in more than 50 nations. They define their field as competitive intelligence—"the legal and ethical collection and analysis of information regarding the capabilities, vulnerabilities, and intentions of business competitors."

Many businesses employ techniques falling well below accepted ethical standards and legality. They use many of the techniques employed by foreign espionage, though without the direct or indirect support of a rival government.

3.5.1 On-the-Ground Intelligence

On-the-ground intelligence is often most beneficial to practitioners of domestic economic espionage. An especially helpful source is a former employee, especially a disgruntled one, who knows the ins and outs of his or her former company. The changing business culture is creating more of these than ever. A couple of generations ago, employees developed close bonds with their employers, and employers made employees feel secure in their jobs. The norm used to be that a college graduate would be hired by a company and then spends an entire career in service to that organization, either working up the corporate ladder or quietly serving in only one professional role.

Times have changed. In recent decades, companies that had been stalwarts of loyalty to their employees discovered that profits could be maximized by encouraging a constant churn of employees, instead of sticking with long-term workers. Long-time employees cost more because they received raises each year, and as they grew older, they also drained the company's healthcare account.

In recent years, with the trend of globalization, companies are finding that they can outsource much of their workforce to nations that have a low-cost workforce. In many cases, these workers have government-paid health plans, and they require few benefits, which drives down their cost even further. The danger is that not only does outsourcing create an even more transient workforce in the United States—it dramatically increases the likelihood that foreign entities will acquire the trade secrets of U.S. companies.

With United States jobs no longer meaning life-long security, employees began to regard their companies as stepping-stones. They no longer considered themselves in service to a company—they considered their job a means to a paycheck, and a disposable means at that. Recent cultural changes have placed less emphasis on teaching ethics, and employees also have less of a desire to stay near family or to remain in one community. The result is a marketplace where employees make job changes every couple of years, and employers who treat their workers as little more than long-term temporary workers. The mixture combines to help employees feel no guilt for jumping to a

competitor company and divulging secrets that will harm their former employer and, consequently, their former coworkers.

Because the clock cannot be turned back, wise employers with trade secrets to protect must require employees at the point of hire to sign a contract that contains penalties for sharing trade secrets and sensitive information after they leave.

Current employees of a business can provide information even more damaging than former employees can. They may do so intentionally—for profit or greed—or they may be tricked into releasing sensitive information, or they may simply make mistakes. Some companies will establish contact with a current employee and bribe him or her into agreeing to be an information source. The employee becomes a mole who burrows into the organization and funnels vital secrets back to the rival business. According to the Xerox white paper, written by former FBI agent Dave Drab, companies are interested in more than executives. Employees much further down the corporate ladder can often get information every bit as effectively as top executives can. Secretaries, technicians—even janitors—can get their hands on sensitive information—especially in companies that do not aggressively limit access to it.

3.5.2 Computer Hackers

Domestic espionage also makes use of hackers to remotely infiltrate a company's computer system, either online or through other means. The 2002 Computer Crime and Security survey revealed the following facts:

- Of the respondents, 90% (mostly large corporations and government agencies) detected computer security breaches in the past 12 months.
- The Internet was cited as a frequent point of attack by 74%.
- Financial losses because of computer security breaches were reported by 80%.
- The worst financial losses came through proprietary information theft at $170.8 million, followed by financial fraud at $115.5 million.

Bibliography

ASIS International. (2004a). Chief security officer guideline. Retrieved July 12, 2007, from http://www.asisonline.org/guidelines/guidelineschief.pdf.

ASIS International. (2004b). General security risk assessment guideline. Retrieved July 12, 2007, from http://www.asisonline.or/guidelines/guidelinesgra.pdf.

ASIS International. (2006). Preemployment background screening guideline. Retrieved July 12, 2007, from http://www.asisonline.org/store/detail.xml?id=59290153.

Department of Justice's Task Force on Intellectual Property. (2006, June). Progress Report of the Department of Justice's Task Force on Intellectual Property. Department of Justice. Retrieved July 12, 2007, from http://www.usdoj.gov/opa/documents/ipreport61906.pdf.

Minieri, M.W. (2004). Protecting corporate secrets: A brief primer on contemporary practices in information security. Reston, VA: Kroll Schiff & Associates. Retrieved July 12, 2007, from http://www.asisonline.org/toolkit/protecting_corporate_secrets.pdf.

4

The History of the SSI Classification System

This guide is not limited to SSI as it relates to the transportation industry. Within the parameters of SSI, this guide will include all information deemed sensitive to our nation, to a business, or to an individual. Over the years, the term *SSI* has grown to encompass a multitude of information types. This chapter will follow the history of other forms of SSI.

4.1 1951: Executive Order 10290

In the interests of national security, the classification system of secrecy has affected crafting of foreign policy, building of weapons, births of entire government agencies, government spending, and play of public debate. It all began in 1951, when President Harry S. Truman signed Executive Order (EO) 10290, entitled "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States."

President Truman believed the purpose of the executive order was to strengthen the safeguards against divulging to potential enemies information harmful to the security of the United States. He said the order "provides, for the first time, uniform standards for classifying and protecting security information throughout the executive branch of the Government."

4.2 1953: EO 10501

Not long after EO 10290 was issued, a special committee convened by former general and president-to-be Dwight Eisenhower—who

was at the time secretary of defense—warned that the classification system was already overloaded, and that proper securing of information that should be protected had suffered. Shortly after winning the presidency, President Eisenhower issued EO 10501, entitled "Safeguarding Official Information in the Interests of the Defense of the United States." EO 10501 was issued on November 5, 1953. This order stated that "it is essential that the citizens of the United States be informed concerning the activities of their government; and … the interests of national defense require the preservation of the ability of the United States to protect and defend itself against all hostile or destructive action by covert or overt means, including espionage as well as military action; and … it is essential that certain official information affecting the national defense be protected uniformly against unauthorized disclosure." The order goes further to describe the classification categories, spelling them out as *Top Secret*, *Secret*, and *Confidential*.

4.3 1966: Freedom of Information Act

In response to the growing concerns over government secrecy, President Lyndon B. Johnson signed into law the Freedom of Information Act (FOIA) in 1966. The law was enacted to deal with requests for government records, consistent with the belief that the people have the right to know about them. President Lyndon Johnson emphasized the FOIA's chief objective: "This legislation springs from one of our most essential principles: A democracy works best when the people have all the information that the security of the nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest."

4.4 1974: The Privacy Act

The Privacy Act of 1974 strengthened the FOIA substantially by covering government documents charting individuals. Exceptions to solicitations of information under these acts are a source of debate. The 9 exemptions to the FOIA and the 10 exemptions to the Privacy Act were controversial when issued, and they remain controversial to this day.

4.5 1977: Presidential Directive (PD/NSC-24)

The legislation surrounding government secrecy versus the public's right to know continued over the years. In 1977, President Jimmy Carter issued a directive (PD/NSC-24) establishing a National Telecommunications Protection Policy. This policy stipulated that "unclassified information transmitted by and between government agencies and contractors that would be useful to an adversary should be protected." The secretary of defense was designated as the executive agent for communications security to "protect government-derived unclassified information," and the secretary of commerce was designated as the executive agent "for communications protection for government-derived unclassified information (excluding that relating to national security)."

4.6 1985: National Security Decision Directive

Subsequently, President Ronald Reagan issued a National Security Decision Directive on September 21, 1985, referring to "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest." However, without further defining such information, the directive ordered that it should be "protected in proportion to the threat of exploitation and the associated potential damage to the national security."

4.7 1987: Computer Security Act

In 1987, the Computer Security Act was passed to improve the security and privacy of sensitive information in federal computer systems and to establish minimum acceptable security practices for such systems. The act defined sensitive information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under … the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

4.8 1992: "CIA Openness"

Then, in February 1992, Central Intelligence Agency (CIA) Director Robert Gates announced the advent of *CIA openness*, promising more media briefings, academic conferences, and documents. In 1993, a scathing newspaper series documenting four decades of nuclear program radiation experiments on unwitting human subjects compelled the Department of Energy to launch its own openness initiative.

4.9 1995: EO 12958

In 1995, the pressure for an end to secrecy had gained momentum, and the first post-cold war president, President Bill Clinton, signed EO 12958. After launching a government-wide review of the country's secrecy policies, he issued the directive to overhaul the classification system of U.S. national security information. The order required the "automatic declassification" of most historically valuable records older than 25 years. The executive order established an interagency review panel with the power to reverse agency classification decisions. In its first 2 years of operation, the panel declassified (in full or in part) more than 80% of the classified records it reviewed—in sharp contrast to past secrecy practices.

4.10 2002: The Card Memorandum

The timeline continues in October 2001, when the attorney general issued a memorandum promising the Department of Justice protection to agencies' assertions of FOIA exemptions "unless they lack a sound legal basis," reversing the Department of Justice's previous pro-disclosure position.

Then, in March 2002, White House Chief of Staff Andrew Card issued a memorandum using the phrase *sensitive but unclassified information*. The Card memorandum, issued to the heads of all executive departments and agencies, directs recipients to "undertake an immediate reexamination of current measures for identifying and safeguarding" government information in their respective department or agency "regarding weapons of mass destruction, as well as other

information that could be misused to harm the security of our nation and the safety of our people."

The Card memorandum also included a memorandum from Laura Kimberly, acting director of the Information Security Oversight Office, calling for agencies to give "full and careful consideration to all applicable FOIA exemptions" in safeguarding "sensitive but unclassified" information. The Homeland Security Act of 2002 mandated information sharing among federal, state, and local authorities, and in conjunction directed the president to "identify and safeguard homeland security information that is sensitive but unclassified."

4.11 2003: EO 13292

On March 25, 2003, President George W. Bush issued EO 13292, amending President Clinton's EO 12958 to "prescribe a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism." Classification levels remained the same. The list of classification categories redefines "scientific, technological, or economic matters relating to the national security" to include "defense against transnational terrorism," and expands a previous category to now cover "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism."

4.12 2005: SBU Information Memorandum

In December 2005, President Bush issued a memorandum for department heads regarding "Guidelines and Requirements in Support of the Information Sharing Environment." In this memorandum, the White House directed the agencies to develop standard procedures for handling SBU information.

It is impossible to account for all legislation pertaining to the history of sensitive information. But keep in mind, this system of secrecy has one ultimate purpose—protecting our nation.

Bibliography

Card, A.H., Jr. (2002, March 19). Memorandum for the Heads of Executive Departments and Agencies. Retrieved from http://www.fas.org/sgp/bush/wh031902.html.

Freedom of Information Act. *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Freedom_of_Information_Act_(United_States) (accessed November 3, 2015).

Kimberly, L.L.S. (2002, March 19). Memorandum for Departments and Agencies. Retrieved from http://www.fas.org/sgp/bush/wh031902.html.

Lawyers Committee for Human Rights. (2003, September). Assessing the new normal: Liberty and security for the post-September 11 United States. Retrieved from http://www.humanrightsfirst.org/pubs/descriptions/Assessing/Ch1.pdf.

The Library of Congress. (2004, September). Laws and regulations governing the protection of sensitive but unclassified information. Retrieved from http://www.loc.gov/rr/frd/pdf-files/sbu.pdf.

The National Security Archive. (2006, March). Pseudo-secrets: A freedom of information audit of the U.S. government's policies on sensitive unclassified information. Retrieved from http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/SBU%20Report%20final.pdf.

Woolley, J. & Peters, G. (1999). The American Presidency Project. Santa Barbara, CA: University of California (hosted), Gerhard Peters (database). Retrieved from http://www.presidency.ucsb.edu/ws/?pid=13925.

PART II
Espionage and Security Breaches

CHAPTER 5 The History of Spies and Espionage
CHAPTER 6 Espionage and Psychology
CHAPTER 7 Spies and Espionage
CHAPTER 8 Social Engineering and Countermeasures
CHAPTER 9 Deception Detection

5
The History of Spies and Espionage

This timeline lists some of the notable moments in the history of spying, focusing on international relationships between countries. Most of the more recent events and spies involve the United States. These examples represent the variety of spies whose work has impacted history, from before Christ to the present day. Many more cases of espionage exist, and many espionage cases may never be discovered.

From the beginning, people and spying have seemed to go hand in hand. Although ancient civilizations did not have the CIA and Komitet gosudarstvennoy bezopasnosti (KGB), those cultures spied within themselves and on each other thousands of years ago.

While it is now common practice for countries to use spies to gain intelligence in and between countries, this practice has a long history that is not confined to modern times.

Although the devices for collecting classified documents have changed with the times, the passing of secret information persists as an area that countries need to address for their protection.

5.1 Espionage in Ancient Times

Deception and theft of information has been around since the dawn of civilization. Before electronic bugging devices, there were eavesdroppers behind curtains. Before written messages, there were secret codes. Before the gun, there was the dagger. Unfortunately, because societies usually like to keep their intelligence gathering operations secret, and most knowledge was communicated through oral traditions, relatively little is known about ancient spies and espionage tactics. Additionally, there is little mention about espionage within the North and South American cultures, although the Inca Empire dominated other cultures for nearly three centuries. It is assumed that

they, and advanced American Indian cultures, engaged in spying and the encryption of sensitive information.

The ancient Egyptians had a thoroughly developed system for the acquisition of intelligence, and the Hebrews used spies as well, as in the story of Rahab. Feudal Japan often used ninja to gather intelligence. Ancient Mesopotamians probably also made use of espionage, as evidenced by the discovery of clay tablets that were clearly meant to protect information by encrypting recipes that were presumably commercially valuable.

Keeping information confidential and out of enemy hands was of great concern to early cultures, which led to the development of the information security technology known as cryptography. Below is a cross-cultural timeline of some early uses and milestones of espionage and information security.

5.1.1 The Bible

Passages from the Bible indicate the use of spies in ancient times. For example, Judges 18:2, 8–9 (New International Version) says, "So the Danites sent five warriors from Zorah and Eshtaol to spy out the land and explore it. These men represented all their clans. They told them, 'Go, explore the land.' The men entered the hill country of Ephraim and came to the house of Micah, where they spent the night…. When they returned to Zorah and Eshtaol, their brothers asked them, 'How did you find things?' They answered, 'Come on, let's attack them! We have seen that the land is very good. Aren't you going to do something? Don't hesitate to go there and take it over.'" Also, Joshua 2 tells the story of Joshua sending spies to Jericho, and in Numbers 13, Moses sends out 12 spies to explore the land of Canaan. When the spies returned, they reported to Moses everything they had seen. These spies were to find out the condition of the land, people, towns, and crops. Other passages include Judges 1:22–24 and Deuteronomy 1.

5.1.2 496 BC

In China, the great military strategist Sun Tzu (544–496 BC) composed his theories into his military treatise, which became known

as *The Art of War*. In it, there is a chapter on the types of spies and their uses. The earliest verified text of this book has dated to between 134 BC and 118 BC. The book contains advice on military strategy, including a chapter on spying. Even today, many people, from sports coaches to politicians, look to the book for its wisdom.

5.1.3 334 BC

Alexander the Great intercepted mail from his soldiers and thus established the earliest known postal espionage system.

5.1.4 350–280 BC

Chanakya, prime minister to the first Mauryan king (ruler of the region of what is now India, Pakistan, and South Asia), is said to have written the *Arthashastra* during his life. The *Arthashastra* (literally meaning "science of political economy") is a treatise of political and diplomatic strategy aimed at uniting India. Along with advice on ethics and an outline of a legal and bureaucratic framework, this collection of writings recommended that a king should employ spies to keep watch on all levels of society. It was added to over the centuries until around the fourth-century BC.

5.1.5 c. 300 BC

During the Etruscan wars, the Roman consul Q. Fabius Maximus employed the use of subterfuge and propaganda to win over local Umbrians to the Roman cause by sending his brother disguised as an Etruscan peasant into the Ciminian forest. The Romans left behind much other evidence and many stories of spies.

5.1.6 50(s) BC

Julius Caesar sent secret messages to his generals and officials using a simple substitution cipher (aptly called the Caesar Cipher) in which each letter in the original text is replaced by a letter some fixed number of positions further down the alphabet. There is no record of any of these messages being successfully cracked.

5.1.7 44 BC

If Julius Caesar had employed more spies, he might have discovered who was plotting to assassinate him and when. He was aware of rumors of a plot to kill him, but he had no further information. He was assassinated on the morning of March 14.

5.2 Espionage: Ninth Century AD–Eighteenth Century AD

5.2.1 Ninth Century AD

Arab mathematician Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi describes frequency analysis in *A Manuscript on Deciphering Cryptographic Messages*. This is the method used to crack substitution ciphers.

5.2.2 AD 54

Early Christians made use of secret codes to avoid persecution. Many historians believe that the number 666 is a reference to the Roman Empire or the tyrant ruler Nero.

5.2.3 AD 240–320

Continued Roman persecution of Christians relied in part on the use of spies to squelch the spread of Christianity.

5.2.4 AD 878

King Alfred the Great disguised himself as a minstrel, wandered through the Danish military camps, and obtained sufficient information to defeat the Danes at Edington. He would later go on to write *The Code of Alfred the Great*, which became the foundation of English common law.

5.2.5 1300s

King Philip used spies to infiltrate the Knights Templar. The Vatican was able to obtain the secret Templar document "Baptism of Fire of

the Brothers-Consulate" (also known as "Secret Rule of the Templar"). With the help of such information and infiltration, the order was persecuted and eliminated.

5.2.6 1420s

The Italian cryptographer Leon Battista Alberti invented the first polyalphabetic ciphers (now known as the Alberti Cipher) and invented a form of machine-assisted encryption using a cipher disk. The polyalphabetic cipher is the use of several alphabets in an encryption. By this period in Europe's Renaissance, frequency analysis was being used to crack codes and undermine national security. However, this cipher was not used properly for several hundred years. It was probably the most significant advance in cryptography since before Julius Caesar's time. Alberti also wrote a treatise on cryptography named *De componendis cifris*.

5.2.7 1424

Emperor Yongle ruled China using eunuchs as spies and appointing them to high positions in government.

5.2.8 1450

The printing press was invented, and it made mass communication and the spread of written propaganda much more efficient.

5.2.9 1558–1663

During the Elizabethan period and at the height of England's Renaissance, Francis Walsingham was the spymaster of Queen Elizabeth and was behind the discovery of many plots to overthrow the queen. Another key espionage figure during this time was Antony Standen, who, according to the British National Archives, "… passed information from Europe to Elizabeth I's 'spy master' Sir Francis Walsingham. His intelligence reports on the Spanish Armada made him a key figure in the Elizabethan secret service."

5.2.10 Late 1600s–Early 1700s

Europe attempted to obtain the secrets of making porcelain from China through the use of spies. At the beginning of the 1800s, such technology appeared. It is unclear if the technology was gained through subterfuge or finally discovered through the process of trial-and-error experimentations.

As we have shown, the use of spies to covertly gather information spans across cultures and throughout human history. Cryptography was developed early in history to protect and communicate sensitive information; and secret codes have been used throughout history to evade political authorities, communicate military secrets, and plot the demise of enemies. Thus, the early histories of these vital facets of civilizations are undeniably intertwined.

5.3 Pre–20th-Century Events

Although it is now common practice for countries to use spies to gain intelligence in and between countries, this practice has a long history that is not confined to modern times. The following exemplify parts of that history.

5.3.1 Daniel Defoe, Born 1660

Although he started out as a merchant, Defoe became famous for his spying skills for England and as the author of *Robinson Crusoe*. He came up with the idea of creating a secret service that observed the citizens of England. He later spied on the Jacobites in Edinburgh, which led to the Treaty of Union in 1707.

5.3.2 The 1700s and the American Revolutionary War

The 18th century brought many technological and philosophical advances that had drastic influences upon society and politics. The 1700s brought the Age of Enlightenment (the intellectual movement that advocated logic and reason), the Industrial Revolution, and continuation of the Scientific Revolution. Military warfare also gained new technology and methods.

A few of the technological advances and important historical events relevant to the topic of espionage and spying include the following:

- Thonius Philips van Leeuwenhoek invented the microscope during the late 1600s, and his discoveries of microorganisms overturned the idea of spontaneous generation of life.
- Isaac Newton gave full accounts of calculus and the properties of optical lenses in 1704. Later, scientists would use such principles to create even more powerful microscopes.
- Continued colonial expansion, including more aggressive settlement of North America, brought about the development of international trade, financial markets, and accumulation of capital.
- The patent law was developed. Lawyers in the English court of Queen Anne (1702–1714) began to require that a written description of the invention be submitted. This would become part of the foundation of modern patent law.
- The widespread use of the musket, bayonet, field artillery (such as cannons), and other firearms in warfare made foot soldiers much more powerful, because almost any man could be given a gun and be taught quickly how to use it.
- War began to be financed through long-term, low-interest loans from national banks, such as the Bank of England.
- The concept of total war appeared. Total war is "a military conflict in which nations mobilize all available resources in order to destroy another nation's ability to engage in war" (Total war, 2007).

These technologies and concepts in the beginning part of the 1700s greatly influenced espionage and the way that intelligence was gathered. It is interesting to note that in 1780s, it was illegal for skilled artisans or manufacturers to leave Britain or Ireland and enter any foreign country for the purposes of practicing their trades. It was also illegal to export many textiles and any manufacturing equipment. This was surely an attempt to curb the theft of information by France and other countries. Rather than break laws by leaving the continent, many tradesmen came in contact with agents and thus foiled the laws. Ultimately, though, for industry such as textiles and manufacturing, which require specialized and delicate machinery, the skills in

assembling such factories were often more important than the plans. Spies were employed in all the wars and conflicts of this era, particularly in the American and French Revolutions. The fundamentals remained the same: to obtain information from the opposition that could be used either in favor of the ruling government or negatively toward the country from where the data had been retrieved.

Espionage, counterespionage, diplomatic sleight-of-hand, propaganda, scouting, partisan warfare, code-making, code-breaking, sabotage, bribery, deception, and disinformation, and other such tactics were used in the American Revolution with outcomes that helped the rebel cause. One example was when the British generals moved to Concord in 1775 because of information from spies that heavy ammunitions were stored there. Colonial agents informed the Americans of the British plans and foiled the British efforts. Another example of the use of spying and counterespionage is in Washington's 1781 use of deception to induce the British side into assuming that there was a French and American assault planned imminently upon New York. While most of the British forces prepared for the attack, Washington proved his military genius by going covertly with Marquis de Rochambeau to defeat Lord Cornwallis at Yorktown in Virginia. The British had been fooled into believing in and preparing for an attack that was nothing more than an American ruse. With British forces so focused on New York, Washington and Rochambeau were able to get to Virginia unnoticed, where their forces met minimal resistance.

5.4 The Revolutionary War

As in every war, when the Revolutionary War broke out, espionage and counterespionage became a necessity. However, the Continentals did not even have an organized army, let alone any type of organized espionage methods to employ against the British. Despite their lack of training in matters both tactical and covert, success depended on the Colonials developing these areas. In a time where colonists were sharply divided between becoming their own entity and staying loyal to Great Britain, nothing was sacred. Neighbors and families were torn apart because of differing viewpoints. It is even thought that while Benjamin Franklin was busy spying on the British for the

Colonials, his son William was spying on him for the British. In light of even intimate relationships being subject to spying, Washington and the Second Continental Congress had to develop systems that would work to combat espionage.

5.4.1 The Culper Gang

It was the embodiment of one of Washington's greatest intelligence dreams. Washington gave the order for Benjamin Tallmadge to design and implement a spy network in New York. Tallmadge took every precaution to protect the identity of the persons in the spy ring and was, in fact, so successful that Washington himself did not know who was in the spy ring. The network consisted of Robert Townsend, Aaron Woodhull, Austin Roe, Anna Strong, and Caleb Brewster. The network was referred to as Samuel Culper, and each person in the network had a different code name that used the surname Culper. The Culper Gang used a complex method of moving information from one person to the next that worked very well the majority of the time. When the letters were intercepted at one point, with the name of someone who wanted to help the colonists, the man was contacted before the British showed up to search his home, and he was able to destroy any information he had before their arrival. After this interception, the Culper Gang began using invisible ink and written code with only Townsend, Woodhull, Tallmadge, and Washington having access to a coded dictionary.

5.4.2 Nathan Hale

If the Culper Gang was one of Washington's greatest intelligence achievements, his biggest failure was undoubtedly Nathan Hale. Hale was given orders by Washington to cross into enemy territory and spy on the British. Hale's mission was clear and he knew what he had to do, but he was poorly trained and was easily tricked into revealing what he was doing by a British Loyalist. He was arrested and hanged on September 22, 1776. Before his execution, he revealed that he did not regret what he had done when he said, "I only regret that I have but one life to give for my country."

5.4.3 Committee of Secret Correspondence

In 1775, Benjamin Franklin, Benjamin Harrison, John Jay, Thomas Johnson, and John Dickinson were appointed to the Committee of Secret Correspondence by the Second Continental Congress. This committee was designed to help establish foreign allies and to gather information from the British that would help the American cause. In 1977, the Committee of Secret Correspondence was renamed to Committee for Foreign Affairs, when the concept of secrecy was no longer deemed necessary following the signing of the Declaration of Independence. The idea that this committee represented was the basic principle upon which the present-day CIA was built.

5.4.4 Benedict Arnold

Benedict Arnold is probably the most famous spy of the 18th century. After fighting in many battles and losing his left leg in battle, Benedict Arnold signed the oath of allegiance to the Colonies. He was, however, bitter about losing his leg and continually at odds with Congress—especially after he was convicted of using government wagons for his personal use and issuing a pass to a ship he later invested in. In 1779, the British offered Arnold more than 10,000 pounds and a military commission to provide military intelligence leading to the fall of West Point. However, the plan was foiled when his courier to the British, Major John Andre, was caught with correspondences and documents in his sock. Andre was put to death for his traitorous activity, but Benedict Arnold defected to the British and escaped. Benedict Arnold died in 1801, having lived the rest of his life undistinguished.

After the United States gained freedom from Britain, there is evidence to support that theft of technology and trade secrets from other countries was, if not encouraged, tolerated. According to the book *Operational Structures of Espionage*:

> Alexander Hamilton argued for a wide variety of measures to encourage business, including the acceleration of ways in which United States companies could acquire the technologies found overseas, and he argued that the United States Congress should work to provide incentives for development of industry across the United States landscape.

5.4.5 Joseph Fouché, Duc d'Otrante, Born c. 1759

Fouché was the minister of police under Napoleon and director of the network that uncovered conspiracies to seize power during the French Revolution. Known for its brutality and strong support of beheadings, his police force kept order while also spying on the citizens of France. Not only did he set up spies, but he also spread false information and used double agents. After being sent into exile for aiding in the death of King Louis XVI, he died in Trieste, Italy, in 1820. He was an inspiration for writers, including Dumas (*The Count of Monte Cristo*) and Hugo (*Les Misérables*), in their creation of evil characters.

5.4.6 Prince Clemens von Metternich, Born 1773

Metternich created an organization of spies in the early 19th century for Austria that kept him informed about Napoleon's actions, all of the members of the Congress of Vienna, and the Russian czar. His spies told him about the czar's plans to have a holy alliance of European nations, and Metternich used this information to implement a plan for a sharing of power among European countries.

5.5 The 1800s: New Inventions

The effects of the industrial and scientific revolutions included many inventions and new technologies. Steam power made railroads possible, and gaslight lit many towns. Of interest to the history of espionage and sensitive information are the inventions of photography, the telephone, and the telegraph (and Morse code).

One of the most important inventions during the early 1800s was that of communication through electric telegraph using Morse code. The longer marks in the code were called *dashes*, and the shorter marks were called *dots*. Morse code quickly became an integral part of aviation and maritime communication. It would become used extensively by the military and during war, persisting through current times.

The first permanent photograph was produced in 1826, but took 8 hours to expose. By 1839, a more permanent process, the daguerreotype, had been invented. New methods of creating photographic

images exploded during this time, and by 1884, the modern technology of film had been developed. Out of this early period also came the cyanotype process—the developed images known as *blueprints*. By using two chemicals—ammonium iron citrate and potassium ferricyanide—light-sensitive coating usable on many surfaces can be made quickly and easily. To develop the picture, it only needed water. This was doubtlessly used in many invisible ink formulas and for assorted documentation purposes.

Finally, at the end of the 1800s, the telephone was invented. Commonly attributed to being invented by Alexander Bell, it was really Antonio Meucci who patented and demonstrated the first working telephone in New York City in 1853. However, Meucci could not afford to file a patent, so in 1875, Alexander Graham Bell received a patent for a similar machine. Antonio Meucci was recognized by the United States as the true inventor of the telephone in 2002.

The technologies and new paradigms of the 17th and 18th centuries gave foundations on which much of today's forensics, espionage, and military tactics still rest. During this period, the modern nation-states were born, as was empirical thought and mass communication. Tools originally intended for benign purposes were later used by spies to gather and spread information for more heinous purposes.

5.5.1 Pinkerton National Detective Agency, Founded 1850

Allen Pinkerton began this organization in Chicago to protect railroad property. Pinkerton gained fame for uncovering a plot to assassinate President-Elect Lincoln and for tracking Jesse James, the Reno Brothers, and the Wild Bunch. The agency is still in existence today as a division of Securitas Security Services USA, Inc.

5.5.2 Okhrana (Department for Defense of Public Security and Order), Formally Organized 1881

The Okhrana was formed to protect the Russian czar. It had been operating since the time of Ivan the Terrible in the 16th century. By spying on the lower class, the Okhrana was able to inform the Czar of planned rebellions. By the beginning of the 20th century, the Okhrana was spying on other countries as well. In 1917, the organization fell

apart when revolutionaries seized the Russian government. Members of the Okhrana were tracked down and killed if caught.

5.6 Civil War Spying

While the origins of the CIA can be traced back to the Revolutionary War, the idea and birth of the Secret Service is directly tied to the American Civil War. When the Civil War began, neither the North nor the South put much stock in spies, let alone had any type of formal intelligence unit. Throughout the course of the war, however, that changed. The spies of this time turned espionage into an art form. The crude, haphazard systems that were being used by both sides early in the war were completely revamped by the end of the war into a smooth, sophisticated system.

The Civil War brought changes in standards for all aspects of war: army size, battle tactics, and, most notably, espionage. At the beginning of the Civil War, neither the North nor the South had a security organization. It was not until toward the middle of the war that both sides began implementing organized security bureaus: the Secret Service in the North and the Signal Bureau in the South. Before the formation of these organizations, generals relied on men and women whom they recruited to gather enemy information and report back. Many soon realized, however, that this was a dangerous endeavor. They were fighting a war where it was exceedingly difficult to differentiate between the ally and the enemy. The mannerisms of a woman from Massachusetts were not entirely different from those of a Virginian woman. A man from Pennsylvania looked just like a man from Arkansas. It was not uncommon for a general to bring a man into his unit, show him around, and tell him what the next maneuver would be, only to find, after the person had left, that they were a spy for the enemy. The similarities between the two sides were not the only weakness that was exploited; the North even used slavery as a weapon against the South. There are many tales of either free blacks, or whites who disguised themselves as blacks, getting placements working in southern homes and camps to obtain enemy information.

Not only were the spies themselves evolving, the technology and methods they implemented were changing as well. In addition to the first organized espionage in this country, the Civil War saw

aircraft-balloons capable of flying over enemy lines and photography utilized by spies. Pictures of enemy camps, maneuvers, and troops were taken and sent back to anxious generals. Even newspapers that would write detailed accounts of the armies' movements and plans were smuggled across enemy lines.

Along with the new technological developments that were being used, both the Union and Confederate armies were using another new weapon: female spies. Although both sides were using male and female spies, the Civil War was really the first war that saw female participation, in any capacity other than nursing, as acceptable. Each side had its fair share of notable male and female spies. Spies for the North included Harriet Tubman, Elizabeth Van Lew, Timothy Webster, and the Dabneys, while the South had Belle Boyd, Rose Greenhow, and Aaron Van Camp.

5.6.1 Harriet Tubman

She is best known for her work helping slaves escape to freedom via the Underground Railroad. Tubman was born a slave in Maryland in 1820. Tubman escaped slavery in 1849, when she fled to Pennsylvania. She spent the next 10 years of her life smuggling slaves from Maryland to freedom in Canada. After her last trip on the Underground Railroad, Tubman became a spy for the Union Army. Tubman was responsible for organizing a group of black men, former slaves who knew the areas she would be infiltrating well, and leading them into enemy territory to obtain information such as locations of ammunition depots, enemy encampments, and cotton warehouses.

5.6.2 Elizabeth Van Lew

Like Harriet Tubman, Elizabeth Van Lew was also a spy for the Union Army. Her espionage days started innocently enough when she was asked to visit imprisoned Union soldiers, bringing them food and medicine. It was during her visits and talks that these soldiers would tell Van Lew of the Confederate troop movements and defense structure that they had observed since being captured. Van Lew, with the help of couriers, passed this information to Union troops. Van Lew also arranged it so that a slave she had liberated, Mary Elizabeth

Bowser, could get a job working for Jefferson Davis, the president of the Confederacy. She would then meet up with Bowser, who would provide her with secretive information about the South's battle plans and relay this information to the Union Army. Although she was an outspoken supporter of the Union Army living in Richmond, she was not seen as a threat by the Confederacy. The people in Richmond called her "Crazy Bet," a name she helped perpetuate by appearing in public unkempt, humming or talking to herself. The people of Richmond are said to have attributed her support of the Union troops to her obvious mental illness.

5.6.3 Belle Boyd

In 1861, 18-year-old Belle Boyd began her career as a spy for the Confederate States when she risked her life to provide pertinent information regarding the Union troops to General Stonewall Jackson. Belle continued her foray into the field of espionage, mingling with Union officers, gathering what information she could from their discussions and reporting back to General Jackson. As time passed, Boyd became more open in her spying for the Confederacy and was arrested twice by Union soldiers. After her first arrest, she was released after only 1 month. Her second arrest, however, kept her imprisoned for more than 6 months. Because of both illness and the public knowledge of her spy efforts, she was no longer able to serve as an effective spy, so instead of staying in the States where she would have been useless, she sailed to England and served as a courier of dispatches.

5.6.4 Rose Greenhow

She was a spy for the South who lived in Washington, DC. She was well known among the members of the high society in Washington and used those contacts to gather information about the Union armies to pass on to General P. G. T. Beauregard. She is most notably credited with supplying General Beauregard with the information regarding the Union troop advance on Manassas. The information she provided prompted the realignment of the Confederate armies leading to their victory at the first Battle of Bull Run. She gained too much attention, however, and was brought under suspicion by Allen Pinkerton

in August 1861. She, like many other spies throughout history, made the mistake of not destroying incriminating evidence, and a search of her house turned up detailed maps and letters. Pinkerton had her arrested, and, although she was imprisoned, she was still able to send messages to Confederate soldiers regarding Union troop activities.

Along with these four individuals, there were many other spies who were active during this time frame—too many to count, really. Some were so successful at adopting their assumed identity that they would be arrested by soldiers for the side of the war they actually represented. Upon confirmation of their identity, these individuals would be released to try again. For all of the lessons learned via espionage during this time, perhaps the lesson with the largest impact was the need to have an organized intelligence operation. The United States government has had an intelligence branch since the inception of the Secret Service.

5.7 Early 20th Century

5.7.1 Mata Hari

Born in Leeuwarden, Netherlands, on August 7, 1876, Margaretha Zelle grew up a privileged child. With a beautiful Javanese mother and a wealthy shopkeeper for a father, Margaretha (who later would become Mata Hari) and her siblings lived in a bourgeois world, sheltered from the world's less pleasant realities. On March 13, 1905, Margaretha became an instant sensation when she took the stage at the Museum of Oriental Art as Mata Hari. Her willingness to appear in scant clothing or nude, as well as her provocative and sexual style of dance, drew crowds from far and away. In fact, it is Mata Hari who is regarded to be the inventor of the strip tease. The Javanese princess then explored Amsterdam, Berlin, Paris, and Vienna, establishing herself as the successful exotic dancer.

The name *Mata Hari* has since served as a trademark for feminine decadence. Mata Hari's beauty and sensuality mesmerized countless men, many of whom were military officers.

As she traveled internationally during World War I, her love affairs with these high-ranking officials transformed into potential business affairs. The combination of crisscrossing Europe and taking to bed both French and German officers raised suspicion by both the Allied

and Central powers. The alleged espionage activities performed by Mata Hari are not conclusive. The theory is that Mata Hari joined the German Secret Service after persuasion by one of her German lovers. She used her dancing to innocently visit various Allied locations, all the while transmitting intelligence reports back to Germany. On October 15, 1917, Mata Hari was executed by a French firing squad. It has been said that she refused a blindfold and even blew a kiss to the 12-man firing squad moments before they shot her dead at the age of 41.

5.7.2 Sidney Reilly

Undoubtedly the world's most extraordinary British spy, dubbed the Ace of Spies, Sidney Reilly is thought to be the inspiration for Ian Fleming's famous fictional secret agent James Bond.

Sigmund Georgievich Rosenblum (aka Sidney Reilly) was born on March 24, 1874, in Odessa, Russia. Born the only son of three children, his father was a wealthy Jewish contractor and his mother a talented pianist. As a young man, he was arrested by the Imperial Russian Secret Police for carrying messages for a student revolutionary group called the Friends of Enlightenment. When he was released, Reilly's assumed father, Grigory, told him that his mother was dead and that his biological father was actually her Jewish doctor, M. Rosenblum (and Grigory's trusted first cousin).

Over a 25-year period, Reilly was involved in, or claimed to have been involved in, a multitude of secret missions. Some of the most significant alleged activities include the following:

- Reilly and Chinese acquaintance Ho-Liang-Shung allegedly stole the Port Arthur harbor defense plans and gave them to the Japanese Navy. With the inside information in the plans, the Japanese Navy launched a surprise attack on Port Arthur, killing more than 31,000 Russians.
- Mr. D'Arcy, founder of the Anglo-Persian Oil Company (APOC), had secured concessions from the Persian government (and was negotiating similar concessions from the Turkish government) for oil rights. Allegedly, Reilly disguised himself as a Catholic priest, boarded Lord De Rothschild's

(of the French banking De Rothschilds) yacht, and secretly persuaded D'Arcy to terminate negotiations to sell his oil rights with the French De Rothschild's and speak instead to the British government.

- At a German air show, one German plane lost control and crashed to the ground. The plane was alleged to use a new type of propulsion magneto. Reilly and a British Secret Intelligence Service (SIS) agent posed as exhibition pilots, removed the magneto from the plane wreckage, and made quick, detailed drawings of the German magneto to report back to British intelligence.
- British SIS sent Reilly undercover to Germany to unearth the new weapons being forged inside Germany's war plants. Reilly arrived in Germany, disguised as a Baltic shipyard worker by the name of Karl Hahn. He obtained a low-level position as a welder at the plant and joined the plant fire brigade. Shortly thereafter, Reilly discovered the location of the weapon plans and broke into the office where they were kept. When the foreman discovered him, Reilly strangled him and completed the theft.
- In 1918, Reilly was sent to Moscow to assassinate Vladimir Lenin or attempt to overthrow the Bolsheviks. However, Dora Kaplan got to Lenin first (although Lenin survived the attempt). Reilly was now a marked man. Outlawed, he was found guilty of espionage and sabotage and was sentenced to be shot if apprehended. He narrowly escaped and returned to England.

Then, in 1925, Reilly was lured back to the Soviet Union, thinking he was meeting with the anti-Communist organization The Trust. Instead, it was a large-scale deception operation powered by OGPU, Stalin's secret police. This time Reilly was captured and put to death in November of 1925.

5.8 World War I: A Proving Ground for Espionage

If there is one thing that spy stories can teach us, it is how much information can be obtained about the enemy, whoever that may be, and how that information can be used to alter the course of events.

The same is true for espionage during World War I. Germany was gathering information about neighboring countries even before the war began. Germans knew the approximate strength of the armies, what countries could be sympathetic to their cause, and what countries would not be seen as a viable threat. Using the information they obtained, Germany was able to dominate World War I early on. Spies were doing their jobs and doing them well. As with other wars, there were several spies who would obtain information and either act upon it themselves or report back to their superiors for them to determine appropriate military action. There were also military officials who were looking for ways to not fall victim to their enemies' spy efforts.

5.8.1 Captain Franz von Rintelen

He was a German spy living in America during World War I. Von Rintelen moved to New York City when the United States was still neutral in World War I. By founding an import–export business, he was able to secure munitions contracts for the allies, turning a sizable profit. His business was not his primary venture, however, merely a front to hide the real reason he was in New York, which was to prevent American ships laden with supplies from reaching the Allies. Von Rintelen used the information he gathered by spying on America along with the information he was able to obtain via his business to know when and where the ships would be accessible. He would then plant incendiary devices on supply ships, not to put people in danger, but to start fires on the ships that would trigger an order to throw ammunition overboard in hopes of saving the ship. Von Rintelen was eventually discovered when one of his German supervisors betrayed him. He tried to escape to Germany but was discovered and detained in England, where he was held until being moved to the United States when it entered the war. Von Rintelen was released in 1920, and he returned to Germany.

5.8.2 Carl Lody

He was another spy for Germany during World War I. Lody began spying for Germany before World War I even began, presenting

himself as a travel guide by the name of *Charles Inglis*, a name he assumed after stealing Mr. Inglis' passport. From his vantage point in Britain, Lody provided information to Germany regarding London's air defenses and Britain's navy. Lody was captured in Killarney and was convicted of espionage when he was found to have incriminating documents in his possession. Lody became the first German spy executed in Britain during World War I and also the first in 150 years to be executed at the Tower of London.

5.8.3 Irving Guy Ries

Irving Guy Ries was another World War I spy to be executed at the Tower of London. Ries, who was using an alias (his real name is not known), was a German spy posing as an American agricultural sales representative. After Ries' arrival in Liverpool, two telegrams were intercepted but allowed through, and Ries cashed them at a local post office. When Ries went to the American Embassy on August 9, 1915, he was looking for a visa so he could travel to Rotterdam; however, the American Vice Consul believed his passport to be a forgery and contacted the police. When Ries returned for his visa on August 10, he was confronted and admitted that, while his passport was forged, his intentions were pure and he did not work for the Germans. The British were not convinced, however, and he went in front of a court martial in September. Although he maintained that he was there only as a salesman, Ries refused to give personal information other than his parents' nationality because he feared he would jeopardize people back in the United States. Ries was found guilty of being a German spy, although there was never any proof that he passed any information to the Germans, and was executed at the Tower of London on October 27, 1915.

5.8.4 Choctaw Code

In late 1918, Germany was making one last major push in the Argonne area, and things were looking bad for the Allies. The Germans had tapped phone lines, broken radio codes, and successfully captured an average of a quarter of the messengers assigned to run between

companies on the battlefield. The one thing Allies did know was that it was nearly impossible to make a phone call without a German spy hearing everything that was being said, thus enabling them to counter any movement that the Allies would make. While walking through his camp, Captain Lawrence (full name unknown) happened to overhear two of his soldiers, Corporal Solomon Lewis and Private First Class Mitchell Bobb, speaking a language that he did not recognize. When asked about it, Lewis told Lawrence that they were speaking the native language of the Choctaw people.

Lawrence quickly established that Lewis knew of at least eight men in the battalion and two headquarters who were fluent in Choctaw. After contacting headquarters there were found to be 14 men fluent in Choctaw. The names of these individuals were Albert Billy, Mitchell Bobb, Victor Brown, Ben Caterby, James Edwards, Tobias Frazer, Ben Hampton, Solomon Lewis, Pete Maytubby, Jeff Nelson, Joseph Okahombi, Robert Taylor, Calvin Wilson, and Walter Veach. These men were then reassigned to ensure that each "field company headquarters would have a code talker." For the duration of the war, these men would both handle and translate any communication, verbal or written, in their native language and then translate it to English for their company commanders. German spies were unable to break the new code, and within 72 hours, the course of the battle had changed for the Allies, and Germany had gone from a seemingly guaranteed victory in the battle to full retreat. The success of the Choctaw Code Talkers was what prompted the use of Navajo as an unbreakable code during World War II.

5.9 Spies Helped Allies Win World War II

Espionage is an ever-evolving process. What worked during the American Revolution would by no means be an effective method in today's world, nor did those methods work during World War II. As with wars before World War II, spies during this war were looking for new and inventive ways to get information from one point to the next. That is exactly what they did. Not only was the means of communication being revamped, so were the spies themselves. From Virginia Hall to Major Martin, spies of World War II were different from the spies who preceded them.

5.9.1 Navajo Code Talkers

Communication of information is imperative in the life of a spy. The biggest problem, as always, was getting this information to its target without anyone else understanding what you were saying. World War I had seen the introduction of the Choctaw Code Talkers. World War II intelligence experts, building off this idea, used the Navajo language to keep information from the Axis forces. Other avenues of relaying information were explored as well.

5.9.2 Unusual Tactics

In September 2006, British security services declassified information pertaining to World War II, including espionage tactics that were used. The information that was released detailed some of the more ingenious methods that spies developed to try to ensure the safe arrival of their messages. Some of the methods listed included hiding codes in sheet music, chess moves, and shorthand symbols (*China Daily*, 2006). Spies would even separate the layers of a postcard, place a thin sheet of paper with notes between the two halves, and then reseal the postcard, successfully concealing the notes (*China Daily*, 2006). The Germans even used fashion to disguise communications. They would hide messages in drawings of models wearing the latest fashions by using Morse code in the detailed stitching and patterns of their clothes (*China Daily*, 2006).

5.9.3 Takeo Yoshikawa, the Pearl Harbor Spy

On March 27, 1941, the Japanese diplomat Tadashi Morimura arrived in Oahu. Little did anyone know that this was a fake identity for Japanese naval ensign Takeo Yoshikawa. His mission was to keep current on the status of the United States fleet and its anchorages, and report his observations to Tokyo by coded telegraph messages. Yoshikawa was to become Japan's only military spy in Hawaii.

Yoshikawa avoided illegally entering military bases or stealing classified documents; instead, he took advantage of America's openness. To evade anti-spy efforts, he relied solely upon memory and assumed that all telephone conversations were tapped.

By mid-1941, Takeo Yoshikawa had given the Japanese military priceless information for its planned surprise attack. He advised the military to choose Pearl Harbor over other sites because the nearly landlocked harbor was deep enough for major fleet units to approach, and it was ideal for an air attack. Yoshikawa used many cover ploys to gather information about Pearl Harbor and other strategic sites: Hickam Air Force Base, Wheeler, Bellows, Kaneohe and Ewa airfields, Schofield Barracks, and Fort Shafter. As tensions increased and security tightened, Yoshikawa kept a low profile, and Japan continued to rely on him for most of its information gathering and reporting. From November 5 to December 7, Yoshikawa sent biweekly *ships in harbor* reports to Tokyo in order to help the approaching Japanese force. Yoshikawa remained in Hawaii during and after the attack on Pearl Harbor. In March of 1942, he and other Japanese were placed in an Arizona holding camp. He never revealed his true identity. Yoshikawa and his fellow Japanese diplomats were eventually exchanged for American officials being held in Japan. Back in Japan, Yoshikawa continued to work in Japanese intelligence until the end of the war. In 1960, he finally told his story to a reporter for *TIME* magazine. Japan had given him neither honors nor pension, forcing him to rely on his wife's income selling insurance policies. He died in 1996 at a nursing home.

5.9.4 Virginia Hall, "the Limping Lady"

Virginia Hall was known by many names: "Marie Monin," "Germaine," "Diane," and "Camille." The Germans gave her the nickname *Artemis*.

She was born in Baltimore, Maryland, and attended the best schools and colleges. She studied abroad in France, Germany, and Austria, finally landing an appointment as a Consular Service clerk at the American Embassy in Warsaw, Poland, in 1931. She hoped to continue her promising career in Foreign Service, but accidentally shot herself in the left leg while hunting in Turkey. The leg had to be amputated and was replaced with a wooden appendage she named *Cuthbert*. She resigned from the Department of State in 1939.

She eventually found her way to England and joined the Special Operations Executive. She spent time in this position stationed in France and became proficient in Morse code. When Germany overran

France, she escaped back to London and was honored as a member of the Order of the British Empire.

Seeking more adventure, she joined the United States Office of Strategic Services and was sent back to occupied France, where she directed guerilla operations and relayed strategic information to London. She found safe houses, mapped drop zones, and trained other resistance forces. For her service in the war, Virginia Hall was given the Distinguished Service Cross, the only female civilian in World War II to receive the United States of America's second-highest military honor after the Medal of Honor.

After the war, she joined the CIA as an intelligence analyst on French parliamentary affairs, where she worked until mandatory retirement in 1966. Virginia Hall died on Bastille Day, July 14, 1982.

5.9.5 The Dead Decoy

Most spies, just because of the nature of their work, spend their time perfecting methods designed to elude capture. There did, however, come a time in World War II when the Allied forces decided that the best way to throw Germany off their trail was to allow one of their spies to be captured with false information in his possession. The Allied forces were attempting to take the island of Sicily when they came up with a plan to avoid giving the Germans time to set up a counterassault when the Allies moved to take the island (Glover, 1998). They knew when they were dropping him off that Major Martin would, hopefully, be captured, as it was a heavily occupied German area. They also knew that Major Martin would not be returning to England alive (Glover, 1998). Nonetheless, he was given an identification, love letters, a picture of a fictional fiancée, and some other personal effects along with documents meant to make the Germans think that the Allies' target was not Sicily, but the island of Sardinia. He was dropped just off the coast Spain with nothing more than a life jacket and these papers in a briefcase cuffed to his arm.

It was soon discovered that Major Martin had been discovered upon reaching shore (Glover, 1998). England demanded his body be returned to England, and when it was, English soldiers noted that his case had been opened and carefully resealed. The Axis powers

immediately shifted their focus to Sardinia, leaving Sicily open to be taken by the Allies. The mission was a success in that Sicily was taken far more easily than had originally been anticipated, with far fewer lives lost, and the Germans never knew the Allied secret. Major Martin would never return to England alive because he was not alive when he was dropped into the ocean. He succumbed to pneumonia back in England and was already dead when he was put on the submarine (Glover, 1998).

5.9.6 The Cambridge Spies

The Cambridge Spies, or The Cambridge Four, was a ring of spies in the United Kingdom who passed information to the Soviet Union during World War II and continued into the 1950s. The four core members met at Trinity University in the 1930s. The ring of four included Kim Philby (aka Stanley), Donald Duart Maclean (aka Homer), Guy Burgess (aka Hicks), and Anthony Blunt (cryptonym: Johnson). Several other people have been implicated as belonging, but not conclusively.

According to crimelibrary.com, these men's personalities were as intriguing as what they did: "The first one, Burgess, was a flamboyant, alcoholic homosexual. The second, Blunt, was a discrete homosexual who rose to knighthood as the Royal Curator of Art. The third, Maclean, was a tense, insecure diplomat of ambiguous sexual persuasion. The fourth, Philby—and perhaps the most intriguing of the group—was a dedicated heterosexual who has been called, not inaccurately, the 'Spy of the Century.'"

After their recruitment at Cambridge, the men were cultivated slowly by Russian Intelligence; thus, their entry into the British Intelligence Service was accomplished without any doubts as to their loyalty. Philby, rather than joining the British Intelligence, became a reporter for the *London Times*.

Between 1940 and 1944, while working in the British Embassy in Washington, DC, Donald MacLean transmitted data on the atom bomb, including its development and progress, as well as the amount of uranium available to the United States. This knowledge, along with the technical information provided by other spies, was responsible for Russia building its own atomic bomb. MacLean was also Stalin's

main source of information about communications and developments between Churchill and Roosevelt.

Philby carried out a variety of assignments, including notifying Russians of the breaking of secret codes, training other spies, and identifying British agents who were sent to Russia.

During World War II, Burgess and Blunt worked in British Intelligence, where they were able to access and then transmit secret Foreign Office and MIS documents that described Allied military strategy.

Ultimately, Russia distrusted the very men it had recruited. According to the British Broadcasting Corporation:

> … So although the KGB had recruited four young Englishmen who appeared dedicated to their cause, was it just possible that the SIS had deliberately placed these men in the path of the Russian recruiter? Was it possible that although the KGB believed that these four agents had penetrated the British establishment, the very opposite was the case—Philby, Burgess, Maclean and Blunt had instead penetrated the KGB? … KGB Officers argued that it had been all too easy for the Cambridge ring. Could the British authorities be so stupid to as to allow men of such left-wing backgrounds into positions of trust in the establishment? How could Philby, who had helped Communists escape from Vienna and had then married a Viennese Communist, get through the security checks that the SIS must carry out on all those it recruited?

Although the Cambridge Four were in positions where the information they gathered could inflict infinite damage, they ultimately were not responsible for as much as they might have been if Russia had fully trusted them.

5.9.7 Gestapo, Formally Organized in 1933

The Secret State Police, or Geheime Staatspolizei, of Germany was organized after the Nazis seized power. The organization operated outside the control of law, allowing the Gestapo power to use brutal force. Although the Gestapo was somewhat successful at catching Allied spies, its members often chased anyone who exhibited the

slightest discontent with the German government. The Gestapo collapsed at the end of World War II.

5.9.8 British Double Agents during World War II, 1940–1945

The British captured almost all the German spies in Great Britain during World War II, and used them as double agents who sent false information back to Germany.

5.9.9 Central Intelligence Agency (CIA), Formally Organized in 1947

The National Security Act of 1947 contained provisions for the creation of the CIA and the National Security Council. The CIA's original mission was to coordinate the United States intelligence activities. The Central Intelligence Agency Act (1949) bolstered the CIA's power by allowing the CIA to keep its budget secret.

5.10 The Cold War

Spies during the Cold War relied on the same tactics that had been perfected previously, even though the information they were gathering was somewhat different. The tactics used remained the same: making use of human weakness via pressure, money, and sex. The information being gathered, however, had changed significantly. During times of war, the most common target for a spy was military movement or planned battle tactics. This was not the case during the Cold War, as there was no real war. The battles were for position. Espionage usually centered on arms race secrets and the design and accumulation of nuclear weapons. Famous names during this time include Alger Hiss, Julius and Ethel Rosenberg, and Markus Wolf.

5.10.1 Alger Hiss—Born in 1904, Trial in 1950

Alger Hiss, born in Baltimore in 1904, served as a key official of the State Department during the formation of the League of Nations in the late 1930s, and he was the secretary general at the 1945 meeting in San Francisco when the United Nations was founded. In 1939, Whitaker Chambers, a former member of the United States

Communist Party, accused Hiss of being a Communist and a spy for the Russians. Although initially seen as laughable, the accusation began to seem more realistic when Chambers claimed that Hiss had given him some papers containing confidential information, and Elizabeth Bentley, an admitted Soviet spy, claimed that she had passed documents to the Soviets from an unnamed government official. As the case proceeded, Chambers produced papers allegedly given to him by Hiss and led officials to rolls of film, which would later be known as the Pumpkin Papers, which he had hidden in a hollowed-out pumpkin. The evidence presented did not result in a conviction for espionage, however. Hiss was imprisoned for 5 years, when he was found guilty of perjury in 1950.

The Hiss case also catapulted an unknown congressman, Representative Richard Nixon, into the national spotlight. Nixon pressed the case against Hiss. Until Hiss died in 1996, he maintained his innocence. It is true that his government position gave him access to professional contacts within the Soviet Union, but no evidence was ever brought forth that definitively identified him as a Soviet spy. The Alger Hiss case is still debated today.

5.10.2 Julius and Ethel Rosenberg—Born in 1918 and in 1915, Respectively; Trial in 1951

They were the married parents of two, and they lived in New York when they were arrested in 1950 for espionage. In a trail leading back to Klaus Fuchs, a scientist in the Manhattan Project and known Russian spy, the Rosenbergs were found guilty of passing information to the Soviets regarding the design of the atomic bomb (Spartacus, n.d.). During the trial, David and Ruth Greenglass, Ethel's brother and sister-in-law, served as key witnesses against the Rosenbergs. David testified that he had been approached by Julius to help spy for the Soviets while he had worked at Los Alamos, and Ruth testified that Ethel was the person who would retype David's handwritten notes for Julius to pass on to the Soviets.

The Rosenbergs maintained their innocence until their execution on June 19, 1953. Since their execution, evidence has been brought forth supporting that Julius Rosenberg was indeed a spy for the Soviets; however, the evidence that convicted Ethel is now thought to

be false. In an interview dated December 6, 2001, David Greenglass admitted that he had knowingly lied about his sister's involvement in his and Julius' activities. He claimed that he had lied when he implicated his sister, stating that he was encouraged by the prosecution to do so at the trial, and he did not care that he had sacrificed his sister for his own family (Spartacus, n.d.). David had also been imprisoned for espionage, but he was released in 1960, 7 years after the executions of his sister and brother-in-law, because he had named names when asked who else was involved in the spy ring, while Julius and Ethel Rosenberg refused to give up the names of anyone else involved.

5.10.3 Markus Wolf

One of the leading spies for East Germany during the Cold War, he had been dubbed *the man without a face* because of his ability to evade being identified for 20 years. Wolf was the head of the Stasi, East Germany's international intelligence division, from 1958 to 1987. Under Wolf's leadership, the Stasi was one of the most effective espionage operations during the Cold War. Instead of targeting those individuals who were higher up in rank, or the secretaries that worked for them, Wolf would target simple sergeants or technical employees. He found that it was possible to obtain more information from these people than from those who might have more of an issue betraying a position of personal trust. Wolf would also encourage the men in his command to look for a government secretary when they needed a woman. In this way, the men could have the companionship they were after but also would have a connection to someone who could procure classified documents and other information. Along with these fairly routine methods of gathering information, Wolf also used some more creative tactics. He identified children that had been born under Hitler's Lebensborn, or master race, program. The children were bred to have blonde hair and blue eyes. They were typically born in clinics and then given up for adoption. The Stasi would have men pretend to be the sons born to the mothers of these children in order to establish presence in the West. When he was interviewed in 1998, Wolf admitted that being a spy denoted a certain lack of morals, but he also theorized that it was the information brought forth by spies that kept

the Cold War from becoming a hot war and, in his mind, the ends justified the means.

5.10.4 Christopher Boyce—Born in 1953, Arrested in 1977; Andrew Lee—Born in 1952, Arrested in 1976

These childhood friends became co-conspirators who sold secrets to the Russians. Mexican officials suspected Lee of killing a police officer, but Lee thought the officials knew he and Boyce were spying for Russia. After torture, Lee confessed and implicated Boyce. Boyce gathered misrouted CIA information from his job at an aerospace firm, and Lee delivered it to the Soviet Embassy in Mexico City for money. After being convicted of espionage and sentenced to 40 years in prison, Boyce escaped and robbed banks in the northwest United States. He served more time and is currently on parole. Lee was convicted of espionage and is out on parole.

5.10.5 The Walker Spy Ring

The word *betrayal* holds many definitions. Throughout his lifetime, John Anthony Walker Jr. betrayed many people in many ways. First, he betrayed his country, "to deliver or expose to an enemy by treachery or disloyalty." He also betrayed the Navy, "to reveal or disclose in violation of confidence." And finally, he betrayed his family, "to deceive, misguide, or corrupt."

We begin with his country. John Anthony Walker Jr. came from a broken home and a troubled childhood. Often in trouble with the law, he was arrested for a petty crime as a teenager. The judge gave him a choice: prison or the United States Navy. Walker joined the Navy, and through his hard work and good efforts worked his way up, eventually earning the rank of chief warrant officer.

While stationed in Boston, Walker met his wife, Barbara Crowley. Although the couple had four children, three daughters and a son, Walker did not give up his philandering, heavy-drinking lifestyle. He often neglected his wife and children, which eventually led to a divorce. His lifestyle ultimately led to financial problems. Walker made many poor investments and was quickly falling into debt. To solve his monetary crisis, he turned to espionage. In 1968, at the

age of 30, he went to the Soviet Embassy in Washington, DC, and offered his services for the purposes of espionage. Walker promised the Russians data on United States encryption devices and top-secret encryption codes that allowed them access to top-secret United States operations and methods. Walker continued to betray his country by selling secrets to the Soviets for more than 18 years. In fact, some say that the KGB considered Walker and the encryption data the most important operation in its history. For his betrayal, Walker earned more than US$1 million for almost two decades of espionage.

Walker also betrayed the Navy. Walker was a member of the United States Navy for more than 20 years, before his retirement in 1976. He began as a radioman and later gained top-secret security clearance for submarine duty, and he eventually became a chief warrant officer. Throughout his naval career, he received large praises from his superiors for his high technical skills and love of the Navy.

But what they did not know was that he was betraying their confidence by selling top-secret information to the Russians. And after his retirement from the Navy, he recruited a Navy senior chief radioman named Jerry Whitworth to join his spy ring. In his position, Whitworth had access to highly classified satellite communications data.

The Navy was the portal through which Walker was able to first commit and then continue his espionage activities.

Walker betrayed his family. His espionage began as a solo mission, but over time, Walker wanted more. And he needed assistance for that to happen. His greed was so large that he recruited his own brother, Arthur J. Walker, a retired Navy lieutenant commander working for a military contractor. Even worse, he recruited his own son, Michael Lance Walker, a yeoman third class. In combination with Whitworth, these three men completed Walker's spy ring, all of whom had varied levels of access to classified information.

Walker also tried to get his daughter, Laura, involved. She served as a communications specialist in the Army, which could have greatly benefited his espionage activities. Laura wisely refused. It was his betrayal of family that eventually led to his arrest. In late 1984, Walker's ex-wife placed a call to the FBI with a tip about his spying. The call was prompted by her concern of the children's current and potential involvement. FBI agents began a surveillance of

Walker based on the tip. After an intensive investigation, FBI agents had gathered the information they needed for an arrest. Agents even witnessed Walker making a drop of classified documents, and found him with a map of clandestine drop points in the Washington area, places where a spy could leave documents to be retrieved by a contact. Walker was arrested and charged with espionage on May 20, 1985.

The spy ring was also uncovered. Michael Walker, Arthur Walker, and Jerry Whitworth were all convicted of espionage. When Michael Walker was arrested, FBI agents discovered 15 pounds of classified materials in his possession. John Anthony Walker Jr. was sentenced to two life terms plus 10 years; Arthur Walker was sentenced to life in prison; Jerry Whitworth was sentenced to 365 years; and Michael Walker was sentenced to 25 years. Michael Walker was released from prison on parole in February 2000.

5.10.6 Jonathan Pollard—Born in 1954, Plea Agreement in 1986

Pollard pled guilty in 1986 to stealing secret information and passing it to Israel for money. As a United States Navy intelligence analyst, much of the information he took still has not been released, making a true understanding of the case difficult. Yet Pollard has insisted that his goal was to protect the security of Israel and not to do harm to the United States. His life sentence is the most severe sentence ever imposed for spying for an ally and is a more severe sentence than many spies receive for crimes against an enemy.

5.10.7 Colonel George Trofimoff

"I hated them [Communists] and so did my whole family."

This statement came from George Trofimoff, the retired Army Reserve colonel who was charged with spying against the United States for the Soviet Union on at least 32 acts. The alleged espionage activities spanned a 25-year-long conspiracy.

Trofimoff claimed he grew up hating Communists and blamed them for the deaths of his family members during the Bolshevik Revolution. He condemned them for killing millions, and he even

joined the U.S. Army to fight them. But the jury did not buy it—Trofimoff was convicted in June 2001 after a 4-week trial and was sentenced to life in prison on September 28, 2001. Trofimoff is the highest-ranking military officer ever charged with espionage.

George Trofimoff was born in Germany to Russian émigré parents. He was raised with Igor Susemihl, also the son of a Russian émigré, and he considered him his brother. In 1947, the two were separated when Trofimoff moved to New York City and enlisted in the United States Army in 1948. Trofimoff found acceptance in the United States and became a citizen in 1951.

Specializing in intelligence work, Trofimoff found a home with the United States Army. In 1953, he received a commission in the Army Reserve, and he was honorably discharged from active duty in 1956.

From there, Trofimoff worked civilian service jobs, and in 1969 became the top United States employee at the Joint Interrogation Center in Nuremberg, Germany, interviewing Soviet bloc defectors and refugees. It was in this capacity that the espionage activities are thought to have begun. Federal prosecutors say Trofimoff's foster brother, Igor Susemihl, who had grown up to become the archbishop of the Russian Orthodox Church in Vienna, recruited Trofimoff for the KGB and served as a courier for thousands of secret records.

Prosecutors say Trofimoff obtained classified information while serving at the Joint Interrogation Center from 1969 through 1994. Trofimoff gained access to all the information received and produced by the Nuremberg center, which included intelligence objectives, priorities for strategic objectives, knowledge of Soviet Union and Warsaw Pact military organizations and capabilities, and knowledge of the current chemical and biological warfare threat posed by the Soviet Union. Prosecutors say that equipped with this highly classified information, Trofimoff photographed the documents, returned the originals, and passed the film to Igor Susemihl or KGB agents. Trofimoff even spoke in a prearranged code to confirm the identity of his KGB contacts when he met them. Prosecutors think more than 50,000 pages of classified documents exchanged hands.

Ironically, the center closed in 1995, the same year Trofimoff retired after 35 years as a civilian Army official. Most details of the center remain classified.

In 1994, German authorities arrested Trofimoff and Susemihl for suspected espionage after Vasili Mitrokhin, a KGB archivist, defected to Britain and identified Trofimoff. However, the case was dropped because of concerns regarding the statute of limitations. With no statute of limitations in the United States for espionage, United States officials continued the investigation.

After a 7-year investigation, United States authorities made their move in late 2000. Posing as Russian officers, undercover FBI agents lured Trofimoff into a sting. Allegedly, Trofimoff felt he was still owed money by the Russians. The FBI used this as bait, offering Trofimoff the money he deserved. When Trofimoff arrived at the West Shore Hilton in Tampa to collect, he was arrested. Before his arrest, Trofimoff met with undercover FBI agents several times and was videotaped fully admitting his past involvement in espionage.

The federal indictment listed the following charges:

- Secretly took classified United States documents relating to national defense away from the Nuremberg Joint Interrogation Center
- Secretly photographed classified United States documents relating to national defense
- Photographed the contents of classified United States documents relating to national defense
- Hand-carried boxes of exposed film to KGB intelligence officers
- Turned over to the KGB photographs of documents from the Joint Interrogation Center that he thought would be of value to the KGB and could not be traced to him
- Received periodic cash payments from KGB officers
- Received cash bonuses from the KGB
- Received about 90,000 Deutsche marks from the KGB
- Used an oral recognition signal or statement, called a *parole*, when he met with a KGB officer
- Concealed from his wife his espionage activities and the true nature of the money he received from the KGB
- Was awarded the Order of the Red Banner

Along with the $250,000, FBI officials say he collected over the course of his spy career, Trofimoff was also awarded the Order of

the Red Banner. This Soviet award is presented for "bravery and self-sacrifice in the defense of the socialist homeland."

The irony was that since 1995 Trofimoff had lived in Melbourne, Florida, on a street called Patriot Drive in a gated community filled with retired military families. On the day of his arrest, the community was flapping with American flags to commemorate Flag Day. And on the day he was sentenced to life in prison without parole, Trofimoff was celebrating the 50th anniversary of his United States naturalization. He gave up a lot for $250,000.

5.10.8 Aldrich Ames—Born in 1941, Arrested in 1994

Aldrich Ames came from a CIA family. His father worked for the CIA, and it was through that connection that Ames was given a summer job when he was 16 years old. In 1962, after graduating from high school and attending for a brief time the University of Chicago, Ames' father helped him once more. He convinced the CIA to hire Ames into the Directorate of Operations to be trained as a spy recruiter. Although he did not prove to be an effective spy recruiter, he did excel at handling spies who had already been recruited by others, earning him a promotion into the position of counterintelligence branch chief in Soviet operations. This position within the CIA gave him access to vast amounts of classified information.

In April 1985, Aldrich Ames found himself nearly $50,000 in debt with no foreseeable way out. When he remembered that one of his subordinates had once been offered $50,000 by the KGB, he decided that he had found his answer. Beginning in December 1984, Ames repeatedly attempted to make contact with Sergey Chuvakhin to offer himself up as a spy for the Soviet Union. For 4 months, he was unsuccessful, but he was finally granted a meeting in April 1985. When he was stood up, he took it upon himself to contact a KGB agent at the embassy, Stanislav Androsov, letting him know that he would be willing to provide him with names of Russian spies who had been turned by the United States in exchange for $50,000. Ames justified his actions by telling himself that the people whose identity he was giving up were double agents sent to the United States by the KGB anyway, so what he was doing was harmless to United States and

Western interests. He also had convinced himself that contacting the Soviets and offering up information for money would be a one-time thing. He would get out of debt, and then never again would he need to contact the Soviets.

Ames did not stop after receiving the initial $50,000. He continued spying for the Russians for another 9 years, ultimately revealing more than 100 covert operations and betraying more than 30 agents, at least 10 of which were executed (CNN.com, 2000, May 29). The only names he refused to give initially were those of 2 agents he had known personally, but while he was stationed in Rome, he gave those names up as well (CNN.com, 2000, June 14). Ames was arrested in 1994, after actively spying for the Soviet Union for nearly a decade. According to an interview with Ames, there was neither glory, need for power, nor a political statement behind his actions; what he did, he did for the money. By the time he was arrested in 1994, Ames had received more than $2.7 million in cash and had another $2 million in Russian accounts waiting for him. Instead of living the life that he had become accustomed to, or even looking forward to retirement, Ames is now leading a different life. He confessed to his crimes, was convicted, and is now serving a life sentence without the possibility for parole.

At the time of his arrest, and for years after, Ames was seen as possibly the most damaging spy in United States history, a role quickly usurped by Robert Hanssen when he was arrested in 2001 for betraying the United States to Russia.

5.10.9 Robert Hanssen

Robert Hanssen was born April 18, 1944, in Chicago, Illinois. He had known from a young age that he wanted to be a spy and even dreamed of "pulling off a caper like the spy in a book Kim Philby, detailing his years as a Russian spy." He was a quiet, intelligent child who never really fit in with his peers. After graduating from high school, he attended Knox College, where he studied chemistry. He then attended Northwestern University after being accepted into the dental school. Tiring of dental school, he changed his major: first to psychology, then finally settling on an MBA in accounting. In 1972, Hanssen joined the Chicago Police Department, just 3 months after

his father retired from a 30-year career. Hanssen was immediately picked up by a new unit, C-5, that was designed to bust fellow officers that were taking bribes from drug dealers.

Three years after taking the position with C-5, Hanssen wanted to move on, so he applied for a position with the FBI. He was rejected the first time, but on January 12, 1976, he was sworn into his new position. After getting his foot in the door at the FBI, he began contacting Russian agents within the first few years, offering to sell them secret information. He made some successful exchanges, and in 1979, was discovered by his wife in the basement of their home, counting the $20,000 he had been given. When his wife questioned him about the money, he told her that he had sold the Russians bad information. Instead of turning him in, his wife forced him to confess what he had done to their priest, who told Hanssen to donate the money to charity. That was supposed to have been the end of it. Hanssen, however, was just getting started.

In 1985, Hanssen wrote a letter to the KGB Chief of Foreign Intelligence, Viktor Cherkashin, offering, again, to sell information for $100,000, this time saying that he would provide original copies so their authenticity would not be questioned. In this correspondence, Hanssen went on to name three Russian officers that were now serving as double agents to the United States. The three names Hanssen gave, Boris Yuzhin, Sergey Motorin, and Valeriy Martynov, were three of the names that had also been given by Aldrich Ames that same year. Martynov and Motorin were captured and ultimately executed, while Yuzhin served 6 years in prison.

Although he claimed to have little need for more money than this initial payment, what he did want was "… to be the best spy ever," so Hanssen continued selling information to the KGB for another 15 years. By many accounts, he accomplished his goal. The information he sold was not limited solely to FBI files. He obtained and sold information from almost every facet of United States Intelligence: the Pentagon, White House, CIA, and National Security Agency. By the time he came under investigation in 2000, it is estimated that he had sold more than 6000 pages of documents and 27 computer disks worth of information and had been given $600,000 in cash and diamonds, plus had an additional $800,000 in a Russian bank account set aside for his retirement. The information he sold

included information regarding KGB assessments and analysis, the FBI Double Agent Program, the United States' plan to protect the president in the event of an attack, and many other top secrets. It is also believed that part of the information he sold may have then been taken by an individual Russian and sold to Al-Qaeda members, who then used that information to avoid being detected before the attacks of 9/11.

Ironically, though he saw himself as "insanely loyal" to his contacts, Hanssen's betrayal was ultimately brought to the attention of the FBI by the very people to whom he had been supplying information. In September of 2000, a former KGB member sold his file to the United States, right down to a trash bag that he had used to secure the information he would leave at the drop-site. The bag had Hanssen's fingerprints. On February 18, 2001, Hanssen was arrested while attempting to leave what was to have been his final drop, complete with a letter resigning from his life as a spy. On July 6, 2001, Hanssen agreed to a deal in which he would plead guilty to 15 counts of espionage and treason, spend life in prison without the possibility of parole, tell the government everything he knew, and be subjected to polygraph tests on demand as long as the government would agree to pay his wife a widow's pension of $38,000 and prosecutors would not seek the death penalty against him. The government accepted the deal and Hanssen was sentenced on May 10, 2002.

5.10.10 Wen Ho Lee

It is one of the most controversial cases involving allegations of spying to date. Wen Ho Lee was born in Nantou, Taiwan, in 1939. At 26, he moved to the United States to pursue an education in engineering. In 1974, he became a United States citizen, and 4 years later, he was hired by Los Alamos National Laboratory in New Mexico as a weapons design scientist. While working in this department, Lee "held a Q clearance, which allowed (him) access to Top Secret information and Restricted Data information" (Wen Ho Lee indictment, 1999). In order to work in this position, Lee signed a detailed document in June of 1987 binding him to secrecy on all information he would receive:

> I (defendant) have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I (defendant) hereby agree that I (defendant) will never divulge such information unless I (defendant) have officially verified that the recipient has been properly authorized by the United States Government to receive it or I (defendant) have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information that such disclosure is permitted. I (defendant) further understand that I (defendant) am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. (Wen Ho Lee indictment, 1999)

Lee hereby stated that he was aware of the potential to cause damage if he divulges information. He also swore that he would "never divulge such information" except in the case of verification by the United States Government. This same government also provided him with the tools and procedures to discern the way in which to handle such classified information:

> I (defendant) hereby acknowledge that I (defendant) have received a security indoctrination concerning the nature and protection of classified information including the procedures to be followed in ascertaining whether other persons to whom I (defendant) contemplate disclosing this information have been approved for access to it, and that I (defendant) understand these procedures. (Wen Ho Lee indictment, 1999)

In December 1999, the FBI accused Lee of spying for China and quickly arrested him. According to his indictment papers, Lee transferred at least 19 files under the *restricted data* or *red* classification to *green* between 1993 and 1994 (Wen Ho Lee indictment, 1999). Under the new classification, any person could access these files. Along with this transfer of information, Lee also deleted more than 360 files from the green classification in January/February of 1999. Among these files were the 19 transferred files from 1993 (Wen Ho Lee indictment,

1999). In all, the indictment charged Lee with 59 counts of failure to correctly handle classified information.

The investigation began when intelligence from the People's Republic of China (PRC) indicated that China had information about the United States warhead W88. The FBI then instigated Operation Kindred Spirit in order to discover who leaked this information to the PRC. Evidence led investigators to focus their attention primarily upon Lee. In March 1999, this evidence in combination with pressure from the United States Department of Energy led the University to fire Lee. The day he was fired, someone leaked his name to the news media, which promptly published information on his case. The news media played an important role in this case, directing both public and federal opinion in opposition to Lee. Its involvement has since come under much scrutiny for swaying opinion. Interestingly, although discovering early in the investigation that Lee could not have had access to the final designs of the warhead, the FBI and the Department of Energy still conducted a full forensic exploration of Lee's office computer.

After his arrest, the government held Lee in solitary confinement from December of 1999 to September of 2000 with no opportunity for bail. In September, he accepted a plea bargain for the United States government and pleaded guilty to one felony count of improperly downloading restricted data. The government then released him from jail, dropping the other 58 counts against him. The importance of this case did not end there. Instead, it is in the post-trial events that many civil liberties groups brought forth accusations of improper behavior on the part of the government and the news media. According to a 2004 *Washington Post* article, U.S. District Judge Thomas Penfield Jackson ordered news reporters to disclose the names of federal officials who leaked Lee's information to the press. Reporters from four organizations were held in contempt for refusing to name their sources (Tucker, 2004). Until they agreed to name their sources, each news organization faced a $500-a-day fine. At that time, Lee himself had a pending civil lawsuit against a *Washington Post* reporter as well (Tucker, 2004).

The debate concerning the role of the media continues. In June 2006, the *Boston Globe* published an editorial commenting on the justice of the case's settlement. The article contended that "neither the $895,000 to be paid by the government nor the $750,000 from the five media outlets can efface the 9 months Lee spent in harsh solitary

confinement." The editorialist notes that the only effort that came close to compensating Lee was the apology made by Federal District Judge James Parker. Overall, the greatest debate in this case has concerned the media's role in defaming Lee's character.

Through many court cases debate has continued among psychologists over the effectiveness and validity of lie detectors. Federal agents used a polygraph test on Lee during his investigation. According to Ken Alder's article "A Social History of Untruth: Lie Detection and Trust in Twentieth-Century America," "In the winter of 2000 … it emerged that agents of the Federal Bureau of Investigation had lied to Lee when they told him he had failed a polygraph test" (Alder, 2002). It seems that it is now commonplace for those who administer the tests to lie to the recipients about their results. Polygraph tests measure "blood pressure, galvanic skin resistance, heart rate, and breathing depth" (Alder, 2002).

These tests fall into wide practice and their results sway juries in many trials. These lie detector results in Lee's case only added to the great number of misrepresented information from other sources in his case. According to Alder, polygraph tests have one major glitch: they require belief on the part of the recipient that they work. If an examinee does not believe that the test works well, he or she can trick the system by controlling his biological responses. In the same way, those who believe in the effectiveness of the polygraph test display truths and lies through their utterances. This difference can be linked to the placebo effect in medicine (Alder, 2002).

Throughout Wen Ho Lee's entire case, much of the controversy arose as a result of the misrepresentations on the part of the media and government. In order to calm the storm after the mishandling of Lee's privacy, the vast majority of the accusations against Lee were dropped. Although Lee breached the security measures to which he signed his secrecy, because of the improper approach to his case, he walked away after his time in solitary confinement with only one count against him. Also, although many of the counts charged against him carried a life sentence, he spent no additional time in jail. Having sued both the United States government and the media for repercussions, he has also published a book, *My Country versus Me*. His supporters decry his treatment by the government and claim that no measures can compensate him for the humiliation his treatment incurred. His

opponents assert that he ought to be thankful for having escaped a lifetime in prison.

5.11 September 11, 2001, and Its Aftermath

The attacks on the World Trade Center and the Pentagon on September 11 by suicidal Islamic extremists will forever be remembered as a dark day in United States history. In all, 2974 people died, not including the 19 airplane hijackers.

Seven days later, on September 18, letters containing anthrax spores were mailed to senators and media officers, infecting 17 people and killing 5. This shut down mailrooms across the country and created even more tension in a nation still coping with the tragedies of September 11. In the immediate aftermath, President George W. Bush declared a war on terrorism. One of the first responses was to freeze bank accounts and financially cut off terrorism. On October 8, he created the Department of Homeland Security in order to strengthen America's protections against terrorism, and he swore in Tom Ridge as the director. Some of the first actions of this new department included tightening visa and immigration policies.

5.11.1 The PATRIOT Act

On October 26, 2001, both the United States House and Senate passed the controversial PATRIOT Act nearly unanimously.

The PATRIOT Act has 10 parts:

- Enhancing security against terrorism
- Enhanced surveillance procedures
- International Money Laundering Abatement and Anti-terrorist Financing Act, 2001
- Protecting the border
- Removing obstacles to investigating terrorism
- Providing for victims of terrorism and their families
- Increased information sharing
- Strengthening criminal laws against terrorism
- Improved intelligence
- Other miscellaneous countermeasures

As is apparent, even from reading the 10 main sections, the PATRIOT Act greatly increased law enforcement's scope and powers. Powers and procedures granted in this act were used to detain people in various facilities, including the infamous Guantanamo Bay detainment camp. Civil liberties activists have debated the necessity of these powers and claim "because the act mandates secrecy about many of its uses, Americans may never know whether their privacy has been violated by law enforcement investigators relying on the act's powers" (Abramson and Godoy, 2007). New civil liberties safeguards were added on December 20, 2005, and the PATRIOT Act was officially amended and reauthorized on March 2, 2006.

5.11.2 United States Departments in Action

After September 11, the focus on terrorism shifted away from domestic terrorists such as Timothy McVeigh and the Oklahoma City bombing, to foreign terrorism. Operation Enduring Freedom began in October 7, 2001, America's invasion of Afghanistan. According to the October 2001 White House Overview of Operation Enduring Freedom, "The United Nations Security Council unanimously enacted a binding resolution requiring all member states to pursue terrorists and those who support them, including financial support systems. The following Departments of United States Government includes 'Actions' taken by them.

1. Department of the Treasury
    - Adoption of Terrorist Financing Executive Order.
    - Froze approximately thirty al Qaeda accounts in the United States and almost twenty accounts overseas.
    - Put 27 names on the Terrorist Financing list.
    - Reviewed additional persons and entities for possible inclusion on the Terrorist Financing list.
    - Froze approximately $6 million linked to terrorists.
2. Department of Defense
    - Approximately 29,000 military personnel, 349 military aircraft, 1 Amphibious Ready Group, and 2 Carrier Battle Groups currently deployed in Theater.

- Approximately 17,000 members of the Reserve have been called to active duty, as well as several thousand National Guards operating under State authority.

3. Department of Justice
   - Analyzed 241 serious/credible threats.
   - Conducted 540 interviews.
   - Conducted 383 searches.
   - Issued 4407 subpoenas.
   - Arrested/Detained 439 persons.
   - Approximately 30 countries offered support in criminal investigations.
4. Intelligence
   - More than 100 countries have offered increased intelligence support.
   - About 150 arrests and detentions of terrorists and suspected supporters of terrorism in over 25 countries.
   - Intensified counterterrorist operations with more than 200 intelligence and security services worldwide."

5.11.3 Weapons of Mass Destruction

On January 29, 2002, in his State of the Union Address, President Bush identified Iraq, Iran, and North Korea as the *Axis of Evil*. He swore that the United States "will not permit the world's most dangerous regimes to threaten us with the world's most destructive weapons." Shortly afterward, on October 10, 2002, use of force against Iraq was authorized and the "president is given authority to take preemptive, unilateral military action against Iraq, when and how he deems necessary. The bill was opposed by 133 representatives and 23 senators" (American Friends Service Committee, 2007). A major reason Congress granted Bush the wide-ranging power to declare war was the expectation that if Saddam Hussein did in fact have weapons of mass destruction, he would not hesitate to use them on the United States.

However, although mustard gas and sarin were discovered (in May of 2004), the conclusion in April was that Iraq had never possessed weapons of mass destruction, which for many was the primary reason to support the Iraq war. According to the Associated Press, "In his final word, the CIA's top weapons inspector in Iraq said … that the

hunt for weapons of mass destruction has 'gone as far as feasible' and has found nothing, closing an investigation into the purported programs of Saddam Hussein that were used to justify the 2003 invasion."

However, this report also stated that Saddam employed many experts, which due to the end of the regime are seeking work. The danger is that hostile foreign governments or other terrorist groups might seek to employ Saddam's former scientists, researchers, and highly trained workers.

The events of September 11 and immediately following will always affect the United States. It was a turning point from which we cannot return. The controversies surrounding our governments and president's actions are still being resolved, and new intelligence is getting discovered frequently. Regardless of how these issues are resolved, it is inarguable that the Department of Homeland Security and the PATRIOT Act have changed the face of intelligence handling and gathering forever.

5.12 Recent History—More Lapses in Security

5.12.1 Sandy Berger

A national security advisor during the Clinton administration, Sandy Berger was caught in 2004 stealing classified documents relating to events leading up to the terrorist attacks of September 11, 2001. Berger had convinced a National Archives executive to let him examine classified documents without going through the proper procedure of reviewing the information under close supervision in a secure room. He was an important person—someone who could be trusted.

In 2003, former President Clinton's National Security Advisor was approached about some files that had gone missing while he was viewing them at the National Archives. Archives rules dictate that someone must be in the same room with persons who are viewing documents and that any notes taken must be reviewed by an Archives employee before removing them from the secure room.

Instead, Berger used personal, private phone calls and trips to the restroom as a means of getting away from the person staying with him, at which time he would put copies of his notes and of top-secret documents into his shirt and pants. Berger would then excuse himself from the Archives, store the documents under a nearby construction

trailer, and then return to the Archives to look through more documents. It was on his third trip that Archives employees became suspicious of his actions and thought he was stealing documents.

When he came in a fourth time, Archives employees had marked documents in order to tell what, if anything, was missing when Berger was done. Going back over the documents, it was found that Berger's focus had been on a report detailing the Clinton administration's handling of a terrorist plot in 1999–2000. He had taken four different copies of this same document. When Archives employees asking about the missing documents first approached Berger, he returned two copies along with his notes saying that he must have accidentally taken them when he was there, and when he had found the other copies among his things, he had destroyed them.

By April 2005, his story had changed, and he agreed to the terms of a plea deal in order to avoid jail time. He admitted to taking the documents, and on September 8, 2005, Sandy Berger was sentenced to pay a $50,000 fine, to serve 100 hours community service, and to pay an additional $6905 to cover the administrative costs associated with his 2-year probation.

5.12.2 Leandro Aragoncillo—Born in 1959, Indicted in 2005

Aragoncillo was indicted in 2005, for what both the FBI and the CIA call the first case of espionage within the White House in modern history. By transferring classified documents by e-mail, investigators say that Aragoncillo passed harmful information about the president of the Philippines to the president's opponents. Aragoncillo is a naturalized citizen from the Philippines who has worked for Al Gore, Dick Cheney, Bill Clinton, and Condoleezza Rice, according to his friends.

Under his plea agreement, Aragoncillo faced up to 20 years in prison. On July 18, 2007, a federal court in New Jersey sentenced Aragoncillo to 10 years in prison.

For information about other notable spies, see the Defense Security Service website at http://www.dss.mil/training/espionage/, which includes information about espionage cases from 1975 to 2004, or the FBI's collection of famous cases at http://www.fbi.gov/libref/historic/famcases/famcases.htm.

Bibliography

Abramson, L. & Godoy, M. (2006, February 14). The PATRIOT Act: Key Controversies. NPR.org. Retrieved July 10, 2007, from http://www.npr.org/news/specials/patriotact/patriotactprovisions.html.

Aiuto, R. The Cambridge spies. Retrieved June 29, 2007, from http://www.crimelibrary.com/spies/cambridge/cambridgemain.htm.

Alder, K. (2002, Autumn). A social history of untruth: Lie detection and trust in twentieth century America. Representations, 1–33.

American Friends Service Committee. (n.d.). Iraq War time line. Retrieved July 10, 2007, from http://www.afsc.org/iraq/guide/war-timeline.htm.

Antony Standen alias Pompeo Pellegrini. Retrieved July 4, 2007, from http://www.nationalarchives.gov.uk/spies/spies/standen/default.htm.

Asoka the Great. (n.d.). Retrieved July 4, 2007, from http://en.wikipedia.org/wiki/Asoka.

Associated Press. CIA's final report: No WMD found in Iraq. Retrieved July 10, 2007, from http://www.msnbc.msn.com/id/7634313/.

Aston, S. (2007). Operational structures of industrial espionage. Retrieved July 5, 2007, from http://www.barracloughltd.com/naag-white-paper.pdf.

Bexte, M. Who was Mata Hari? The story of famed courtesan Mata Hari. Retrieved June 2006, from http://sc.essortment.com/whowasmatahar_rhrc.htm.

Bock, N.A. (2002, October 11). War powers granted. SuffolkJournal.com. Retrieved July 10, 2007, from http://www.suffolkjournal.com/news/2002/pages/warpowers.htm.

Bowcott, O. (2002, September 7). How fate, and Stalin, finally dealt the "ace of spies" a losing hand. Guardian Unlimited. Retrieved July 2006, from http://www.guardian.co.uk/uk_news/story/0,3604,787632,00.html.

Case. Annapolis, MD: Naval Institute Press, 1999.

Castro, J. (1985, June 3). Betraying Navy—And country; A former officer and his son are charged with spying. Retrieved October 2006, from http://www.time.com/time/magazine/article/0,9171,957749-1,00.html.

Chachere, V. (2000, June 14). Top military man alleged to be spy. Associated Press. Retrieved August 2006, from http://www.infobeat.com.

China Daily (2006, September 5). Britain reveals how Nazi agents hid messages in models. Retrieved June 6, 2007, from http://english.people.com.cn/200609/05/eng20060905_299642.html.

China from Mongols to the Ming. Retrieved July 4, 2007, from http://www.fsmitha.com/h3/h12china.htm.

CNN.com. (2000, May 29). CIA spy hunter talks about notorious turncoats. Retrieved October 2006, from http://archives.cnn.com/2000/US/05/29/cia.spy/index.html.

CNN.com. (2000, June 14). Retired United States Army Reserve colonel accused of selling secrets to Soviet Union. Retrieved August 2006, from http://archives.cnn.com/2000/US/06/14/military.espionage.03/index.html.

Deac, W. (1997, May). Takeo Yoshikawa: World War II Japanese Pearl Harbor spy. *World War II Magazine*. Retrieved June 29, 2007, from http://www.historynet.com/wars_conflicts/world_war_2/3035811.html?page=2&c=y.

DeArmond, P. (2002, August 16). The anthrax letters. *Albion Monitor*. Retrieved July 10, 2007, from http://www.monitor.net/monitor/0208a/anthrax.html.

Dougherty, L. (2000, June 15). Retired colonel accused of spying. *St. Petersburg Times*. Retrieved August 2006, from http://www.sptimes.com/News/061500/TampaBay/Retired_colonel_accus.shtml.

Duelfer report. (n.d.). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Duelfer_Report#Duelfer_Report.

Fact sheet: Civil liberties in the USA PATRIOT Act Conference Report. (2005, December 20). Retrieved July 11, 2007, from http://www.usdoj.gov/opa/pr/2005/December/05_opa_682.html.

Fact sheet: USA Patriot Act Improvement and Reauthorization Act of 2005. (2006, March). Retrieved July 11, 2007, from http://www.usdoj.gov/opa/pr/2006/March/06_opa_113.html.

From Republic to Emperor Augustus. Retrieved July 4, 2007, from http://www.fsmitha.com/h1/ch18.htm.

George Trofimoff. Retrieved August 2006 from http://www.videofact.com/english/trofimoff.html.

George Trofimoff press release. (2000, July 14). United States Attorney's Office, Middle District of Florida. Retrieved August 2006, from http://cicentre.com/Documents/DOC_Trofimoff_Press_Release.htm.

Glover, V. (1998). Dead spies tell no tales. Retrieved June 6, 2007, from http://brevia.com/Main/thespy.htm.

Goler, W. (2004, May 17). Sarin, mustard gas discovered separately in Iraq. Fox News. Retrieved July 10, 2007, from http://www.foxnews.com/story/0,2933,120137,00.html.

Guantanamo Bay detention camp. (n.d.). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Guantanamo_Bay_detention_camp.

H.R. 3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled as Agreed to or Passed by Both House and Senate). Retrieved November 3, 2015, from http://thomas.loc.gov/cgi-bin/bdquery/z?d107:hr03162:%5D.

Haines, G.K. (1994, Winter). Virginia Hall Goillot, Career Intelligence Officer. *Prologue: Quarterly of the National Archives*. Vol. 26, No. 4: 249–260. Retrieved June 29, 2007, from https://www.cia.gov/kids-page/6-12th-grade/operation-history/world-war-ii.html#virginia.

Herrington, S.A. (1999). *Traitors among Us: Inside the Spy Catcher's World*. Novato, CA: Presidio.

History of cryptography. (n.d.). *Wikipedia.* Retrieved July 4, 2007, from http://en.wikipedia.org/wiki/History_of_cryptography.

History of patent law. (n.d.). Retrieved July 5, 2007, from http://en.wikipedia.org/wiki/History_of_patent_law.

http://www.quotationspage.com/quotes/Mata_Hari/.

Hunter, R.W. & Hunter, L.D., eds. (1999). *Spy Hunter: Inside the FBI Investigation of the Walker Espionage*. Annapolis, Maryland: Naval Institute Press.

John Anthony Walker. (n.d.). *Wikipedia.* Retrieved October 2006, from https://en.wikipedia.org/wiki/John_Anthony_Walker.

Knightly, P. (2003, April 15). The Cambridge Spies. Retrieved June 29, 2007, from http://www.bbc.co.uk/history/worldwars/coldwar/cambridge_spies_01.shtml.

Laytner, R. (2007). The last samurai. Edit International. Retrieved June 29, 2007, from http://www.editinternational.com/index.php?pag=stories.php?cat=3f5121f82466f&sub=417fbd79e1454.

Lytle, T. (2000, June 15). Brevard retiree is accused of espionage. *The Orlando Sentinel*. Retrieved August 2006, from http://www.fas.org/sgp/news/2000/06/os061500.html.

Mata Hari. (n.d.). *Wikipedia*. Retrieved June 2006, from http://en.wikipedia.org/wiki/Mata_Hari.

Mata Hari timeline. Retrieved June 2006, from http://www.twoop.com/people/mata_hari.html.

Morse code. (n.d.). *Wikipedia*. Retrieved July 5, 2007, from http://en.wikipedia.org/wiki/Morse_code.

Navy 1985–1989: John Anthony Walker. Retrieved October 2006, from http://www.dss.mil/training/espionage/Navy2.htm.

Nguyen, D.P. (2001, June 22). Trofimoff: I grew up hating Communists. *St. Petersburg Times*. Retrieved August 2006, from http://www.sptimes.com/News/062201/Worldandnation/Trofimoff__I_grew_up.shtml.

Pinkham, M.A. The Templars' biggest secret and the Vatican. Retrieved July 4, 2007, from http://www.gnostictemplars.org/articles/Article_-_The_Templars_Biggest_Secret_and_the_Vatican.pdf.

Polmar, N. & Allen, T. Mata Hari. *Spy Book: The Encyclopedia of Espionage*. Retrieved June 2006, from http://www.randomhouse.com/features/spybook/spy/961113.html.

Pravda, online. (2005, April 11). Soviet secret police tricked British spy into a trap 80 years ago. Retrieved July 2006, from http://english.pravda.ru/main/18/90/362/16415_sidneyreilly.html.

Reilly, Ace of Spies. Retrieved July 2006, from http://www.crimelibrary.com/terrorists_spies/spies/sydney_reilly/index.html.

Rise and fall of the Mauryan Empire. Retrieved July 4, 2007, from http://www.fsmitha.com/h1/ch13.htm.

Schräpel, B. FemBiography Mata Hari. (Translated from German by Niederhauser, J. & Horsley, J.). Retrieved June 2006, from http://www.fembio.org/women/mata-hari.shtml.

Sheldon, M.R. (n.d.). Espionage in Ancient Rome. Retrieved July 4, 2007, from http://www.historynet.com/magazines/mhq/3028426.html.

Sidney Reilly. Retrieved July 2006, from http://members.tripod.com/chipress/chipress/reilly.htm.

Sidney Reilly. Retrieved July 2006, from http://www.reference.com/browse/wiki/Sidney_Reilly.

Spartacus. (n.d.). Sidney Reilly. Retrieved July 2006, from http://www.spartacus.schoolnet.co.uk/SSreilly.htm.

Stewart, L. (2000, April). Industrial espionage and technology transfer; Britain and France in the eighteenth century. *Canadian Journal of History*. FindArticles.com. Retrieved July 5, 2007, from http://find-articles.com/p/articles/mi_qa3686/is_200004/ai_n8899680.

Term paper on the history of counterespionage in the United States. Retrieved July 5, 2007 from http://www.termpapergenie.com/counterespionage.html.

The Age of Enlightenment. (n.d.). *Wikipedia.* Retrieved July 5, 2007, from http://en.wikipedia.org/wiki/Age_of_Enlightenment.

The History of the Bank of England. (n.d.). *Wikipedia.* Retrieved July 5, 2007, from http://en.wikipedia.org/wiki/Bank_of_England#History.

The Industrial Revolution. (n.d.). *Wikipedia.* Retrieved July 5, 2007, from http://en.wikipedia.org/wiki/Industrial_Revolution.

The Lives of the Caesars, The Deified Julius, (written c. 110 CE). Retrieved July 4, 2007, from http://www.fordham.edu/halsall/ancient/suetonius-julius.html.

The spy who loved chemistry. Retrieved July 2006, from http://www.chemsoc.org/chembytes/ezine/2002/cook_dec02.htm.

The USA Patriot Act, Preserving Life and Liberty. Retrieved July 11, 2007, from http://www.lifeandliberty.gov/highlights.htm.

Time line of events related to September 11th. Retrieved July 10, 2007, from http://www.patriotresource.com/wtc/timeline.html.

Time magazine. (1985, November 11). Belated concern: Walker pleads for his son. Retrieved October 2006, from http://jcgi.pathfinder.com/time/magazine/article/0,9171,960320,00.html.

TimeLine: 300 to 201 BCE. Retrieved July 4, 2007, from http://www.fsmitha.com/time-bc6.html.

Tom Ridge sworn in as Director of Homeland Security, White House East Room, Washington, DC. October 8, 2001 10:53 A.M. EDT. Retrieved July 11, 2007 from http://www.patriotresource.com/wtc/president/oct/011008a.html.

Total war. (n.d.). *Wikipedia*. Retrieved July 6, 2007, from http://en.wikipedia.org/wiki/Total_war.

Tucker, N. (2004, August 19). Wen Ho Lee reporters held in contempt. *The Washington Post*.

Various authors. (1885). Meucci's claim to the telephone. *Scientific American* Supplement, 520. Retrieved July 5, 2007, from http://www.gutenberg.org/files/13401/13401-h/13401-h.htm#13.

Weapons of mass destruction. (n.d.). *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/WMDs.

Wen Ho Lee indictment. (1999). FindLaw. Retrieved from http://news.findlaw.com/legalnews/lit/lee/index.html.

Who served here? Benedict Arnold. Retrieved July 5, 2007, from http://www.ushistory.org/valleyforge/served/arnold.html.

Who's who: Mata Hari. (2001, December). Retrieved June 2006, from http://www.firstworldwar.com/bio/matahari.htm.

6

Espionage and Psychology

JANET MIELKE SCHWARTZ, PhD, DABFE, DACFM, DABPS, FACE, CHS III

6.1 Development of the Office of Strategic Services

The Assessment of Men (1948) is a great book that documents the activities of the group that was the forerunner of the CIA in America. It is the true story of the development and implementation of a brilliant assessment program that selected spies during World War II from 1944 through 1948. This book allows the reader to view the psychological profile of a spy from a historical perspective of spy assessment. The book chronicles the well-grounded, disciplined work of the well-trained and capable psychologists and psychiatrists who, while inexperienced in the discipline of psychological assessment, made their way through the created process even as they were caught up in the passion of the World War II era. The committed group of psychologists and psychiatrists were the staff of the Office of Strategic Services (OSS) Intelligence Service , later to become known as the CIA.

The ambitious team was led by two compatriots: the dynamic master creator, Henry "Harry" Murray, and his colleague, Major William "Wild Bill" Donovan, who was chief of the OSS. Donovan's historical significance is intriguing. Franklin D. Roosevelt ran against Donovan in the race for governor of New York. Roosevelt, the victor, respected and liked Donovan, who had been the commander of the Fighting Irish regiment in World War I and had been decorated on several occasions for his heroic actions. Together, Murray and Donovan provided examples of leadership and initiative that served to enhance the likelihood of a successful work effort. The task at hand was to determine individuals who would become successful spies. Before

this time, pencil and paper selection tests were utilized and had been found to be ineffective in predicting a skillful spy, as stated:

> The organization has been recruiting too many men who have intelligence and the necessary mechanical training but who lack common sense, know nothing about working with men or how to look after the welfare and the morale of men under them. We simply must have men who can shoulder responsibility and use initiative with common sense. Simply because a man has intelligence does not qualify him for this type of work. In some instances we also have had men who fall into the class of high strung or emotional type. We simply cannot use men of that type in the field when they have to live with Chinese, eat Chinese food, and be under pressure at times. In most cases these men have suffered nervous breakdowns and other nervous ailments. (OSS Assessment Staff, 1948, p. 2)

6.2 Mission and Purpose of the OSS

The mission and purpose of the OSS program was to select and train spies, to train people to conduct destructive operations behind enemy lines, to disintegrate the morale of enemy troops, and to encourage the focus of the underground (OSS Assessment Staff, 1948, p. 10). The task to be accomplished by the OSS team was extremely difficult, because those doing the selecting had little information regarding the jobs or the cultural setting within which the candidates would be expected to perform.

6.3 The Making of a World War II Spy

6.3.1 General Variables and Characteristics

Seven general variables were determined to be essential to the selection process:

- Motivation for the assignment
- Energy and initiative
- Practical (effective) intelligence
- Emotional stability
- Social relationships (e.g., teamwork)

- Leadership
- Security (ability to keep secrets, discretion, ability to bluff)

Three additional characteristics were added for other critical jobs:

- Physical ability
- Observing and reporting (accurate recall)
- Propaganda skills

6.3.2 The Recruiting Process

6.3.2.1 Pre-Selection The recruits were pre-selected and had been referred from various sources by their supervisors because of a perceived level of excellence. Each had been sent a copy of the general instructions, which reviewed the procedures to be followed as well as an assortment of information, including specific instructions to report to a building on the corner of 24th and F streets in Washington, DC. Upon arrival, they were briefed and led to the basement of the corner building, where they removed their outer clothing and destroyed all identification marks on their underwear. They each received two sets of army fatigues, changed into their assessment uniforms, boarded a paneled truck, and were told that they were being sent to the country, where they would be asked many questions and given a number of tests by a group of psychologists and psychiatrists (OSS Assessment Staff, 1948, p. 62).

6.3.2.2 Relocation Recruits were informed that they would be incognito during their stay at the assessment center, and that they were not to talk about themselves or say anything that would reveal their true identity. Any photographs, letters, or items marked with initials would need to be left behind. They were instructed to choose a name by which they would be known during the assessment period. And so it was—two times a week, groups of 18 carefully screened candidates descended on the assessment center known as *Station S*, a country estate on 186 acres in the rolling hills of Virginia.

Upon arrival, they were given a warm and gracious welcome in a social setting. An "informal, sincerely genial atmosphere at the assessment station was established. It was believed that under these

conditions most of the candidates would enjoy themselves and be more inclined to tolerate an exacting and stressful schedule of procedures than they would be in a less agreeable social climate" (OSS Assessment Staff, 1948, p. 33).

6.3.2.3 Evaluation Once the unsuspecting recruits were in place, the three-and-a-half day selection process began. Each of the 10 assessment variables mentioned earlier was measured using an assortment of measurements, including various intelligence and personality tests, a psychosomatic inventory, a health questionnaire that evaluated a wide range of factors, a work conditions survey, a very detailed personal history form, the Belongings Test (in which they viewed a supposed psychologist's personal living area who needed to leave quickly—the task was to make inferences from the 26 personal effects set up in the room), the Brook and the Wall (situational tests requiring the ability to solve a physical logistics problem), structural tests that were designed to tap emotional stability and frustration tolerance, an in-depth personal interview during which both statements and behavior were studied, and a culture-sensitive test called the Office of War Information (OWI) Test (which assessed one's potential to administer propaganda). The OWI test was administered to the entire group at once.

The test lasted 20 minutes. Each candidate was given a single sheet of paper at the top of which was typed the following hypothetical assignment and question: Suppose you have been placed in charge of propaganda activities for OWI in Korea, to work out a program designed to win Koreans over to our side, what information would you want to have? (Assume that you know nothing about the country. Omit administrative questions of staff, finances, and OWI policy. Use outline form if you prefer.) (OSS Assessment Staff, 1948, p. 122).

Additional measures of evaluation included a map memory test, a mechanical comprehension test, a test of observation and memory, the Manchuria Test (for the purpose of measuring the candidate's propaganda skills), and a discussion session during which the recruits were observed as they attempted to be verbally resourceful. And, lastly, there was a stress interview or interrogation test, which was to determine the candidate's ability to tolerate extreme measures of emotional and intellectual strain.

> Each candidate was given 10 minutes to invent an innocent cover story for having been caught without a pass, reading a secret file in a government building at 9 p.m. Then the candidate was led to the basement and pushed into a chair lit by harsh lights shining directly into his or her eyes, to be aggressively grilled. (Handler, 2001)

The stress interview was then immediately followed by the post-stress interview.

Designed with the intention of attempting to catch the candidate off guard to determine whether or not he or she would break cover, each was informed that he or she had failed the test. Their responses to receiving this information yielded unique and significant data.

Additional situational tests and observational tests followed during the subsequent hours and days—an obstacle course exercise occurred as well, psychodrama followed by a debate, a sociometric questionnaire was given that sized up other candidates, a test that involved investigating a mock murder mystery, and a baseball game. During each activity, the style, content, and adequacy of the candidate's performance was carefully rated by a minimum of one, but usually two or three staff members (Handler, 2001).

6.3.2.4 Final Selection During the late morning of the fourth day, the 18 candidates were returned to Washington, DC, in the same panel truck in which they had arrived. It was then that the OSS staff began to prepare for their staff conference, during which they selected those who were deemed as capable and qualified to serve as a spy.

6.4 Exploring the Mind of a Spy

Spies who betray their own country have long been perceived as a more unusual type of criminal than those typically involved in other kinds of crime. However, a new perspective may be considered. Treasonous spies do not merit special regard or a special classification. On the contrary, these individuals may be regarded as merely being another variety of white-collar criminal who just became involved in matters of national security (Stone, 1989). Some theorize that however serious the consequences of their acts, the behavior of spies who perform

espionage against their own country may best be understood as having similar motivations to other greedy white-collar criminals. The public's perception has been that nearly all American spies that have been caught had been motivated by money. But, is this an accurate assumption?

In an article published in *The Boston Globe*, Adam Pertman explores "why they spy" and concludes that the common denominator today among "people who export their nation's secrets" is best described by a Hollywood screenwriter's line: "Show me the money" (Pertman, 2001). Others, such as FBI analysts, psychiatrists, and researchers, agree that rationales ranging from disenchantment with specific government policies, feeling disgruntled with their own jobs, problems with self-esteem, living out fantasies of a more flamboyant lifestyle, or experiencing a loyalty conflict (cognitive dissonance) due to one's ancestry or religion may be among the array of reasons which prompt men and women to act out the betrayal.

> "People usually spy for some combination of emotional gratification and remuneration," stated John Pike, the director of GlobalSecurity.org, a Washington-based policy organization. "But, whatever their reason, in almost all cases today, money is how people keep score." (Pertman, 2001)

Scientific effort has been made to develop a two-factor theory or model for motivations that led to traitorous spy behaviors. One researcher identified a bipolar effect with money (or greed) at one end and ideology at the other (Stone, 2001). Discussions with past or present government-employed counterintelligence officials led him to conceptualize an additional orientation, that of being disaffected. One becomes disaffected or dissatisfied with how one's self has been treated by others, including organizations or political entities. A continuum was created wherein *disaffected* is at one end, and the opposite end was labeled as *other*, being representative of some kind of other orientation, meaning concern for the welfare of others. Stone (2001) suggests that either two-factor motivational theory, i.e., money or greed versus ideology or disaffection versus other may be a means to understand the motivation of treasonous spies. To test his theory, Stone assembled the research facts of

175 United States spies identified since the end of World War II (note: additional reports claim the number to be ranging from 98 [Gelles, 2006] to 150 [Edwards, 2001]), and was significantly able to place a total of 153 United States spies on either of the bipolar dimensions (Stone, 2001):

Money (greed) _____ Ideology
or
Disaffection_____ Other

6.4.1 Project Slammer

In 1985 (Pertman, 2001), United States intelligence agencies embarked on a 10-year benchmark study named, *Project Slammer* (Air Force Special Programs Security Education Council, 2006), which was focused on interviewing 30 incarcerated spies. The purpose of the study was to determine the motivation of the convicted spies and to learn the methods by which they committed their crimes. Although dated, the previously classified study's findings remain significant, and so do its conclusions:

- No offender entered a position of trust with the intent to betray.
- There were two prevalent personality traits.
- They were highly manipulative, dominant, and self-serving.
- They were passive, easily influenced, and lacking self-esteem.
- A large number were substance abusers.
- Their decision to betray was based, in part, on their belief that their coworkers would not report them.
- They were male (note: several women have committed espionage on the United States; these statistics reflect only those spies interviewed as part of Project Slammer).
- Marital status was irrelevant.
- Those interviewed were immature, with an inability to cope.
- Interviewees had an antisocial personality.
- There were significant personality changes that started suddenly with behavior change throughout (Air Force Special Programs Security Education Council, 2006).

Bertram's (2001) analysis of the principal findings of the Slammer Study was that a particularly detailed traumatic event provided the impetus for an individual's eventual decision to cross the line. And, although the 30 subjects of the study were initially terrified about being caught, their fear gave way to euphoria (Bertram, 2001). They felt no guilt about their betrayal while they were conducting the espionage, and even sometimes after being arrested, because they participated in self-deceptive rationalizations (Gelles, 2006, p. 4).

The United States government has extensively studied the behaviors associated with the risk of espionage, and Project Slammer was one interagency project where a team of federal agents, along with government psychologists and psychiatrists, interviewed the convicted spies: focusing on their motivation and the methods they utilized in their search to understand the behavior, motivation, complete mind-set, and personality of the spy; security and counterintelligence professionals hoped to learn enough information to improve the early identification and treatment of employees at risk for committing serious offenses.

6.4.2 Personality Disorders

According to Gelles (2006), betraying one's country does not result from an isolated moment of uncontrollable insight. It results from a long process or emotional crisis. And, typically, the at-risk behavior has not been observed or reported by a colleague or superior. Spies may not fit the current perception of crazy, but they usually are emotionally disturbed, suffering from one or more personality disorders. The two most commonly experienced being the antisocial personality disorder and the narcissistic personality disorder.

6.4.2.1 Antisocial Personality Disorder The antisocial personality disorder is manifested in behaviors reflecting a tendency to reject the normal rules and standards of society. Individuals of this orientation experience a focus only on what they can get now, with little interest in the future and no focus on learning from the past. They are not capable of forming deep friendships, deep attachments, or developing a commitment to anyone or anything. Their capability to remain loyal is severely compromised.

Most people with an antisocial personality disorder have criminal records that make them ineligible for security clearances, many milder versions are eligible and do receive clearances. While on the job, they "press the limits of rules and regulations to see how much they can get away with, and bend the law when it conveniently accommodates their self-interest. Professionally smooth and glib, the similarities with white-collar criminals are startling. They have much capability to be convincing and to talk their way out of trouble" (First & Tasman, 2004, pp. 1246–1249).

6.4.2.2 Narcissistic Personality Disorder Narcissistic personality disorder traits include unmerited feelings of self-importance or self-esteem (grandiosity), feeling entitled, and a general lack of empathy for others. Many successful individuals or overachievers have what appear to be narcissistic traits, i.e., a big ego. However, from the security perspective, a concern arises only when an individual's view of his or her own abilities is so distorted from reality that he or she becomes aligned with a destiny of disappointment rather than success (First & Tasman, 2004, pp. 1257–1261; Gelles, 2006, p. 2).

When confronted by criticism or a failure, such individuals feel devalued by the individual or the organization and may react with a temper tantrum or, perhaps, extensive written appeals. A narcissist's relationship with others may turn very quickly from love to hate or vice versa, depending on whether the relationship supports or minimizes the individual's compelling need to validate a grandiose self-image.

Narcissists who feel rejected and underappreciated by their organization or supervisor need to defend themselves against strong feelings of inadequacy. Their responses may be passive aggressive, vindictive, or generally rebellious. To balance the devaluations, he or she might turn to a foreign intelligence service to satisfy emotional needs, finding enormous satisfaction in working as a spy and outsmarting the organization that rejected him or her (Gelles, 2006, p. 2).

6.4.3 Three Critical Factors and Traits Lead to Treasonous Betrayal

Although antisocial behaviors and strong narcissistic tendencies are frequently associated with increased security risk, these tendencies

need not lead to a more serious offense. Gelles (2006) cites three critical factors that necessarily must be in position in order for a trustworthy and loyal government employee to cross the line and participate in the activities of a spy.

6.4.3.1 Character There must be a personality or character weakness such as antisocial tendencies or narcissism that causes a predisposition to maladjusted, counterproductive behavior.

6.4.3.2 Stress A personal, financial, or career crisis puts an individual with these weaknesses under great stress, triggering more obvious counterproductive behavior often observed by friends, coworkers, or a supervisor.

6.4.3.3 Lack of Intervention The friends, coworkers, and supervisor fail to recognize the signs of a serious problem and decide they do not want to get involved, or assume that someone else will take care of it. As a result, no one intervenes to help resolve the problem, and the individual's behavior spirals out of control.

Most spies have an inability to accept responsibility for their own actions. Mistakes are minimized or ignored, and they blame others for their problems (Gelles, 2006, p. 3).

6.4.4 Positive Qualities Create a Strong Capacity for Loyalty

Screening recruits and potential employees for the ability to accept criticism without defensiveness, an ability to express anger and frustration appropriately, feeling compassionate and being considerate to others, showing respect for the rights of others, the ability to work collaboratively and cooperatively with others to achieve a common goal, and having a strong social support system is essential. Self-discipline in delaying gratification in order to achieve a long-term goal, keeping one's work, honoring commitments, and recognizing that one is not entitled or owed anything from life, but that one must work for whatever one gets, are also ideal qualities to look for (Gelles, 2006, p. 3).

6.5 Categories of Spies

Three categories of spies will be generally discussed: spies committing espionage within the United States government, spies within white-collar organized crime activity, and agents of radicalization, particularly in the growing concern of homegrown terrorism. While the reader may be most familiar with government spies, other emerging areas of criminal and destructive activity have developed their own systems of spying in order to achieve the determined goals.

6.5.1 Government Spies

According to a 1995 General Accounting Office Report (the last year for which full data were available), more than 3.2 million federal and contractor employees held security clearances in 1993 (Figure 6.1).

Obviously, there is great potential for future spies who may be similar to the infamous John Walker, one of the most damaging spies of all time, who had significant gambling debts (Pertman, 2001); Jonathan Jay Pollard, who spied for Israel out of solidarity with fellow

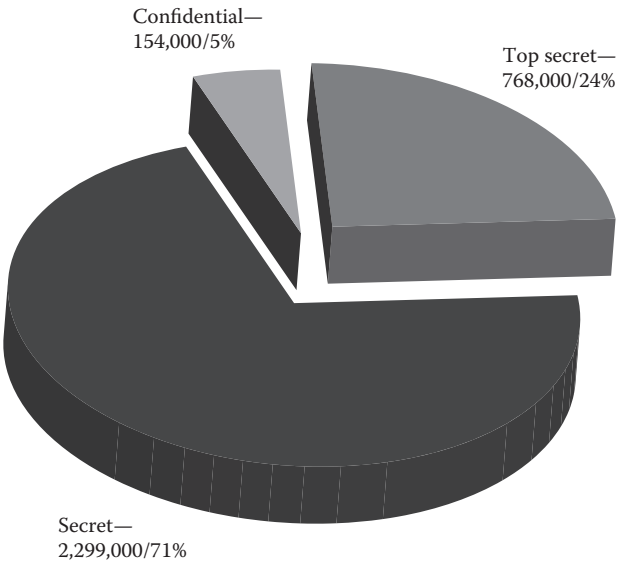

Figure 6.1 Security clearances by classification.

Jews and because of his family's enormous loss of 70 lives during the Holocaust (Blitzer, 1989, as cited in Pollard: Grandiose imagination, 2006); Aldrich Ames, the 31-year CIA veteran, whose multiple character weaknesses of alcohol abuse, arrogance, grandiosity, and impulsiveness were manifested as he compromised over 100 intelligence operations against the Soviet Union (Unclassified Abstract of the CIA Inspector General's Report on the Aldrich Ames Case as cited in Pollard: Grandiose imagination, 2006); Robert Hanssen, the devoted Catholic and member of the Opus Dei, who, in his role as an FBI counterintelligence expert, was accused of selling secrets to Russia for 15 years (Edwards, 2001; Pertman, 2001); or Earl Pitts, former Future Farmer of America, Army captain, and FBI agent who sold out his country and the Bureau for $224,000 during 7 years of secretly spying for the Russians (Thomas, 1997).

6.5.2 White-Collar Crime Not Involving Spies

For purposes of clarification, three categories of white-collar crime do not seem to thrive on spy contacts, as listed below:

- Personal or ad hoc crimes—The offender has no face-to-face contact with the victim (income tax violations, credit card fraud, some kinds of identity theft, affinity fraud, or investment scams that use religious, ethnic, or professional affiliations to gain the trust of victims), fraud against government entitlement programs, etc.
- Abuses of trust—The offender usually acts alone; he or she is in a position of trust or power over specific assets and abuses the privilege (embezzlement, creating ghosts on the payroll, using one's employer's property or information for private profit, and some cases of identity theft
- The con artist and the con man (Schwartz, 2005)

The categories of white-collar crime that rely on spies (followers) to enhance the activity have been referred to as white-collar organized criminals and the white-collar organized community. Organized crime is defined as "two or more people who get together to commit a criminal activity that offers them the maximum profit with the least amount of detection" (Clark, 1994).

Based on continued research of more than 150 semistructured interviews of victims, alleged perpetrators, perpetrators, and their wives, behavioral characteristics have been determined for both of these categories (Schwartz, 2005). White-collar organized criminals are specialists in short-term plans, but are poor in regard to long-term plans. They look for followers (spies) who provide information and also perform tasks in order to belong, as well as to experience approval from the community's power structure. Vulnerable individuals, such as members of certain ethnic groups eager to gain community acceptance, may be particularly susceptible to this coercion. Others likely to become followers might be those who need money for back taxes, gambling debts, keeping up with social pressures, an illness in the family, needing the favor of a recommendation from an influential person in order for one's child to gain acceptance at a prestigious university, the expenses associated with having a mistress, etc. These are some common reasons why individuals sell out to the establishment running the game in town (or, the county).

Research indicates that controlling by fear, bribes, and influence assures a steady stream of followers that are willing to persist. Expert at rationalization, one adapts well to playing the game, mistakenly assuming that this is the way to gain increasing success. The followers are groomed for inclusion, similarly, as one is inducted into a cult (Schwartz, 2005). Spinning a broad web of bribery and intimidation over time will profoundly alter a community's social and moral values.

6.5.3 Agents of Radicalization

Steven Emerson, executive director of The Investigative Project on Terrorism, testified to the United States House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment (Emerson, 2006) regarding forefront issues of homeland security. Each incidence of radicalization within Muslim populations in Western societies is unique, but commonalities have been noted including a charismatic spiritual leader, mosque attendance, Internet connection, and overseas travel.

Homegrown terrorism, a growing trend (*New York Times*, 2006), poses unusual challenges to law enforcement, as before the incident,

the newly radicalized individuals had not necessarily appeared as extremists. Emerson (2006) warns against the misleading notion that those who befall radicalization are individuals who are disaffected, or feel marginalized in some way. While this, indeed, may be true in some cases, there are more prevalent descriptors that have been the impetus for one's indoctrination toward extremist ideology.

Emerson identified underlying characteristics common to homegrown terrorism:

- Those involved appear to lead normal lives, at times even after indoctrination into an extremist ideology.
- Those involved come from an array of backgrounds, but they are largely first- or second-generation Americans with a Middle Eastern or South Asian ethnic origin. The significant role played by Islamic converts is apparent in the cases of the *Virginia jihad network*, the recent Canadian plot, the Folsom prison case, the Portland Seven, and the London bombing cell.
- The majority of these radicalized individuals who become involved in such plots are under the age of 30 and are often radicalized in private study circles or by individuals they meet at their place of worship.
- In several instances, an older and charismatic imam, or spiritual leader, is involved, such as Ali Al-Timimi or Juma al-Dosari in the United States; and in the case of the Toronto plot, Qayyum Abdul Jamal, a 43-year-old mosque volunteer from suburban Toronto. These homegrown jihadists are often well integrated into Western society, and many were students at American universities.
- Certain domestic radical Islamic civil society groups engender radicalization through spreading a false sense of persecution and alienation in the Muslim community in the West, labeling the War on Terrorism a war on Islam. In nearly all of the post-9/11 terrorist plots, unsuccessful and successful, the perpetrators have claimed that they are only avenging crimes committed by the West against Muslims.
- The effect the Internet has on radicalization and the formation of homegrown cells has increased exponentially. Experts around the world agree that access to the Internet is having

a radicalizing effect on Western second-generation Muslim youth, who find themselves divided between two cultures with contrasting value systems. The Internet can facilitate the entire process of the development of a plot, from initial radicalization to the formulation of a complex and potentially deadly terrorist attack (Emerson, 2006).

6.6 Indicators of a Growing Problem

Research conducted by the Defense Personnel Security Research Center (Kramer, Heuer & Crawford, 2005) discovered 10 critical trends that are relevant to espionage involving the theft of classified as well as proprietary information, and that also pertain to the unlawful transfer of documents, materials, and/or other information to foreign, rather than domestic, recipients. According to Director James A. Riedel, the study (Kramer, Heuer & Crawford, 2005) examined situational factors that affect the frequency with which insider espionage will occur.

The converging of global economic competition, the information revolution, the development of new interference of intelligence, and other factors of change in the domestic and international environment have created ample opportunity for insider espionage. Those most capable of exploiting organizational assets at the greatest expense to American interests are permanent, temporary, and former employees, vendors, suppliers, and contractors.

The study has found that technological advances in information storage and retrieval are dramatically improving insiders' ability to access and steal classified and proprietary information:

- The global market for protected United States information is expanding. American insiders can sell more types of information to a broader range of foreign buyers than ever before.
- The internationalization of science and commerce is placing more employees in a strategic position to establish contact with foreign scientists, businesspersons, and intelligence collectors, and to transfer scientific and technological material to them.

- The increasing frequency of international travel is creating new opportunity for motivated sellers of information to establish contact with, and transfer information to, foreign entities. Foreign buyers have greater opportunity to contact and assess the vulnerabilities of American personnel with access to protected information.
- Global Internet expansion is providing new opportunities for insider espionage. The Internet allows sellers and seekers of information to remain anonymous and provides means by which massive amounts of digitized material can be transmitted to foreign parties in a secure manner.
- Americans are more vulnerable to experiencing severe financial crisis because of aggressive consumer spending habits and other factors. Financial problems are a common source of motivation for insider espionage. The increasing popularity of gambling and the prevalence of gambling disorders suggest that greater numbers of insiders will commit workplace crimes such as espionage to pay off debts and to sustain gambling activities. Because organizational loyalty is diminishing, fewer employees may be deterred from committing espionage out of a sense of obligation to the agencies and companies that employ them. Changing conditions in the American workplace suggest that greater numbers of insiders may become motivated to steal information from employers to exact revenge for perceived mistreatment.
- More insiders now have ethnic ties to other countries, communicate with friends and family abroad, and interact with foreign businesspersons and governments. Foreign connections provide insiders with opportunity to transfer information outside the United States, and foreign ties can provide motivation for doing so. More Americans view human society as an evolving system of ethnically and ideologically diverse, interdependent people and groups. This is highly beneficial in many respects, but it is also possible that some insiders with a global orientation to world affairs will, under extreme circumstances, view espionage as morally justifiable if they feel that sharing information will benefit the world community (Kramer, Heuer & Crawford, 2005).

6.6.1 Government Spies

A coworker or supervisor's decision to report or not to report often determines whether a spy will be caught or get away. Watch for new signs of anxiety produced by financial stress, depression, or alcohol or another substance abuse, and report the changes to the appropriate personnel. Observing irregularities in correspondences or communications, unexplained income, excessive use of the photocopier, and removing classified information from the office are other details that raise suspicion. Choose to act, and make a difference.

The security office personnel may then be able to intervene and perhaps even help the employee before an act of espionage occurs ("Walker was intrinsically evil").

6.6.2 White-Collar Organized Crime Activity Spies

There are many safeguards to protect and insulate yourself from coercive tactics, subtle though they may be, that draw you into espionage: value truth, justice, fairness, and doing the right thing; develop independent and critical thinking skills; learn to respectfully question; if personal issues include fearing conflict or being alone, work on these issues to prevent vulnerability; avoid organizations, workplaces, or individuals who indicate how to think (if you object, you are out); develop a mindfulness—beware of community "lieutenants" that seek followers; cultivate mental, emotional, and spiritual fortitude; avoid illusions, i.e., needing to see everyone as pure when they are not; trust your intuition; hold others accountable and report unusual details or findings to authorities; and, finally, live with principles.

6.7 Concluding Remarks

The Economist, a weekly periodical, issued a special report that assessed America's and Britain's intelligence reform (*The Economist*, 2005a) and strongly urged more change. The report acknowledges that governments are known to build up their intelligence services, but then heap scorn on them for their mistakes, their likelihood to violate laws, and to put it very simply, get it wrong.

Despite the gross number of errors in the past 25 years, more money and more power have accompanied the demands for reform. Now is the time to regain a bright new focus and work to strengthen our intelligence services. Of the three largest intelligence services in the world, America still ranks first and is then followed by Great Britain and Russia. The reorganizational tasks ahead will require leadership that is effective, energetic, and capable of great initiative. (Remember *The Assessment of Men*?) Consider these recommendations from *The Economist* report:

- Double-check all systems to see whether the information or material is authentic. Assessments need to be challenged with critical thinking and not just accepted.
- America has fallen into the habit of relying too extensively on high-tech surveillance. Spying is not merely a high-tech science.
- Communicate, rather than compete, with each other.
- Non-partisan oversight will lead America forward.

On the organizational details, the director of National Intelligence is in charge of 15 agencies including the CIA. Surprisingly, the CIA receives only 10% of the budget; the largest intelligence budget is provided to National Security, under the jurisdiction of the Department of Defense. Agencies must be held accountable, and in the trickle down, employees and supervisors need to be held accountable (*The Economist*, 2005, pp. 13, 29–31).

A Senate report, investigating the Iraq situation, found America's spies "negligent and incompetent" (*The Economist*, 2005, p. 31) because of patterns of groupthink (failing to re-examine received information); CIA analysis that was seldom double-checked; detection of dual-purpose materials that was taken as proof of programs in existence; and ambiguous pieces of intelligence that were compiled together to reach a very specific conclusion (layering). The report's conclusion was that our intelligence system was not working well because of a broken corporate culture and poor management—problems that surely would not be solved from additional funding and personnel (*The Economist*, 2005, p. 31). Further, organizational reform will not correct problems resulting from language barriers. Half of the CIA's case officers are in

Baghdad, but only a handful are fluent in Arabic. Most must interview Iraqi interpreters and remain in the green zone.

The critics are harsh in their assessment, but change has already been in process for more than a year. Reform will take place; each small step will lead to a more solid step. Each strong decision will lead to an effective system that values accountability and a best practices fit. Let us wish our nation's new intelligence leaders well. May our own work reflect the high standards we set for them. Above all, believe wholeheartedly in the mission and purpose of this meaningful and interesting work.

Never fear, it can be done.

Bibliography

Air Force Special Programs Security Education Council. (2006). Security educator's news: Personnel security. Retrieved October 28, 2006, from http://www.dss.mil/training/sec_news.pdf.

Ames: Too many weaknesses. Retrieved October 3, 2006, from http://rf.web.tamus.edu/security/secguide/Spystory/Ames.htm.

Clark, J. (1994). Meeting of Manhattan FBI High Intensity Drug Trafficking (HIDTA) Program, July 26, 1994, at 2 p.m. at 26 Federal Plaza, Manhattan, New York City.

Commission on Protecting & Reducing Government Secrecy. (1995). Final Report to Congress, Chapter 4: Figure 3. Retrieved October 28, 2006, from http://www.dss.mil/seclib/govsec/chap4htr.66k.

Edwards, B. (2001). Profile: Possible motivations of alleged spy Robert Hanssen, as reported by Barbara Bradley on *Morning Edition* on National Public Radio.

Emerson, S. (2006, September 20). *The Homeland Security Implications of Radicalization*. Testimony before the United States House Committee on Homeland Security Subcommittee on Intelligence. Information Sharing and Terrorism Risk Assessment.

First, M.B. & Tasman, A. (2004). *DSM-IV-TR Mental Disorders: Diagnosis, Etiology & Treatment*, pp. 1246–1249. New Jersey: John Wiley & Sons, Ltd.

Gelles, M. (2006). *Exploring the Mind of a Spy.* Naval Criminal Investigative Service. Retrieved October 3, 2006, from http://rf-web.tamu.edu/security/secguide/Treason/Mind.htm.

Handler, L. (2001, June). Assessment of men: Personality assessment goes to war by the Office of Strategic Services Assessment Staff. *Journal of Personality Assessment*. Vol. 76, No. 3, pp. 556–578. Retrieved October 13, 2006, from http://web.ebscohost.com/ehost/detail?vid=42&hid+2&sid=f32b904b-0656-4e46-8003-aa4c9e6e.

Kramer, L.A., Heuer, R.J. & Crawford, K.S. (2005). *Technological, Social, and Economic Trends That Are Increasing United States Vulnerability to Insider Espionage*. Defense Personnel Security Research Center, Monterey, California.

New York Times. (2006, October 10). Public Broadcast System. "Frontline," Program presented by the *New York Times* as an update on terrorism.

OSS Assessment Staff. (1948). *Assessment of Men: Selection of Personnel for the Office of Strategic Services*. New York: Rinehart & Co.

Pertman, A. (2001, February 2001). Why they spy: Be it ideology, ego or disaffection, almost always a thread connects motive and money. *The Boston Globe*. Retrieved October 3, 2006, from http://www.fas.org/sgp/news/2001/02/bg)22501.html.

Pollard: Grandiose imagination. (2006). Retrieved October 3, 2006, from http://rf.web.tamus.edu/security/secguide/Spystory/Pollard.htm.

Schwartz, J.M. (2005). *Psychology of White Collar Criminals*. Lecture on ongoing research to the Association of Certified Fraud Specialists National Conference in San Francisco. Permission granted to the United States Department of Justice Executive Office for United States Attorney's Office of Legal Education to videotape the presentation. September 29, 2006.

Stone, L.A. (1989). On the psychological makeup of a spy. *Forensic Reports*, Vol. 2, pp. 215–221.

Stone, L.A. (2001). *A Two-Factor Motivational Theory for Spying Behaviors* in *Psychology of Espionage Reports*, Vol. II. Retrieved October 3, 2006, from http://www.home.earthlink. net/~lastone2/espionagearticle3.htm.

The Economist. (2005a, March 19). The spy game: The use and abuse of secret agencies. Vol. 174, No. 8418, p. 13.

The Economist. (2005b, March 19). Special Report: Intelligence Reform. "Can spies be made better?" Vol. 174, No. 8418, pp. 29–31.

Thomas, E. (1997, July 7). Inside the mind of a spy. *Newsweek*. Vol. 130, No. 1, pp. 34, 2p, 3c.

Walker was intrinsically evil. Retrieved October 3, 2006, from http://rf.web.tamus.edu/security/secguide/Spystory/Walker.htm.

7
Spies and Espionage

7.1 Profile of a Spy

When security is intentionally breached, it is usually a spy of some kind that inflicts the damage. The government's sensitive information is of course under constant attack from spies inside and outside the United States. Business, too, must thwart spies who seek to steal trade secrets or customer databases. An individual must be wary of identity thieves who use espionage tactics to obtain identification numbers.

Spies today come in all shapes and sizes, and their espionage takes many forms. Remove from your mind all images of James Bond or Jason Bourne. Spies do not usually wear tuxedoes, nor do they swagger around with shaken-and-not-stirred martinis clutched in one hand and an impossibly beautiful woman held in the other. They may not necessarily be any more physically fit or attractive than you, and most all of them do not have licenses to kill.

They look like anyone you might meet. Some may be balding and obese. Some might be very old, and some very young. Expect foreign government agents to be so average you would never pick them out of a crowd. That is their intention.

A spy could be an agent of a foreign government or an employee of a foreign or domestic business. A spy could be someone sitting in the next cubicle—a person who probably never thought he or she would ever go into espionage. But the situation was right, and there were unfulfilled needs to be met.

You cannot tell spies from looks alone. But you might be able to identify them by their behavior. That is what the following sections are all about.

7.2 A Double Life

Ibrahim I. Chalhoub, PhD

Spies lead a double life. Those who live as spies for a long time can handle the extreme pressure of having a multitude of statuses and roles, unrelated to each other and kept in complete secrecy from one another, no matter how close a relationship is in effect. Spies are highly trained and meticulously prepared.

Take a closer look at what a real spy is. First, by nature, a spy is an extreme model of contradictions. At the basis of a spy's personality lies a loyal traitor. They are contradicted by the opposing forces of heroic aspiration versus being unknown as an undercover operative, and are, thus, unknown hero.

Isolation causes strain on the individual. If a spy is caught, he or she is completely left alone. The spy will be killed either by captors or by employers neutralizing the possibility of information leakage, despite how trained the spy is.

In contrast with Voltaire's principle that "humans are good by nature," Sigmund Freud clearly states that the unconscious—the driving force of every human being—is a mixture of all evil wills. Freud's theory is supported by the concept of the *unknown hero*, which ensures the satisfaction of the masochistic component of personality. The eternal conflict of the *eros* (life instincts) and *thanatos* (death instincts) causes humans to have a constant struggle between preservation and self-promotion and the sadistic and masochistic components of their personality.

Winning the struggle of thanatos against eros in the concept of unknown hero thus satisfies the masochistic component. The hero coming from eros (with its sadistic trait) is neutralized by being unknown, as if not existing (through self-destruction, thanatos). The struggle is demonstrated in modern, pop culture representations of spies, such as the scenario of the attractive hero charming the opposite sex through many relationships. However, promiscuity can be dangerous, for more reasons than one, and definitely should not to be promoted even though the behavior of satisfying the human sex drive is another way of satisfying the sadistic component of the personality.

A spy is a mysterious person, but with increased extreme internal (as well as external) conflicts, a spy is no more than a human being whose forces of the unconscious can be clearly explained.

7.3 Types of Spies

Spies vary in their motives, types of information gathered, and methods. They are generally employed by government, private sector, or independent motivation. Depending on the specific framework, spies can be categorized in different ways. For the purpose of this section, we will use the organization based on the legendary Chinese military strategist Sun Tzu's book, *The Art of War*:

- Local spies—Outsiders who possess insights of the opposition.
- Internal spies—Ranked officers or personnel within the organization of the opposition.
- Double spies—Enemy intelligence operators who are under a home nation's employment.
- Dead spies—Expendable enemy intelligence operators who are under our employment. Their primary role is to spread disinformation within the organization of the opposition.
- Living spies—Living spies are enemy intelligence operators (who are under a home nation's employment) that are positioned for a specific situation to create maximum damage within the organizational structure of the opposition (such as "returning with significant intelligence" or "setting up someone to spread disinformation").

There are two main reasons to have insights into the different types of spies, according to the book *Secrets of Computer Espionage: Tactics and Countermeasures*, that is, to understand the technical capabilities and limitations of a potential adversary. This is obvious because you want to make sure that your own security measures can withstand a spy's attempt to breach them.

So you can put yourself in the spy's shoes. This is so that you can better assess your own security in order to fully protect yourself; however, you need to know not only the tools and the techniques, but also the mind-set of a spy.

Popular culture has the saying, "What would _____ (Jesus, Gandhi; fill in your favorite wise role model) do?" When you review your security, you need to ask, "What would a corporate spy (or whichever type of spy may be a threat) do?"

Sun Tzu is reported to have said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

7.3.1 Local Spies

Local spies are outsiders who possess insights into the enemy. Governments may question new immigrants, journalists, and refugees in order to gain knowledge about their target. For corporate espionage, trade shows and job fairs can be valuable sources for local spies, and recently fired and laid-off employees from the competition can often provide priceless information.

At the independent level, a job seeker may schmooze acquaintances in order to get them to divulge information about their companies by giving the job seeker an edge on getting hired in the position and for the organization the person seeks.

However, local spies are often biased to the point of being useless. According to the Time.com article "Judging Spies and Eyes":

> … Information gathered from local spies is considered especially unreliable in Central America, where passions run deep and tips are often twisted Complains one United States intelligence official: "The level of emotion in the information we receive is pretty high."

A goal in using local spies should be that of converting higher-ranking officials into internal spies.

7.3.2 Internal Spies

Internal spies are often referred to as *moles*. These are the high-ranking individuals within an organization who are converted into working for the opposition. They are often the most dangerous type.

According to industry surveys, such as the 2000 Computer Crime Report by the FBI and the Computer Security Institute, insiders are considered to be the biggest threat to computer security. Seventy-one percent of the companies surveyed have experienced unauthorized

access by insiders. This implies that corporations, government agencies, and research institutions are increasingly vulnerable to insider espionage.

In the corporate world, internal spies are responsible for untold damage. Employees may spy for competitors because of a variety of motives. The desire for financial gain is very strong, as is the desire for revenge in motivating personnel to divulge company secrets to competition. Existing employees also have access to equipment and computers, and can tip off competitors about security weaknesses or install monitoring devices. The possibility of internal spies wreaking irreparable damage provides strong motivation for the employer to be aware of who is accessing what information and why.

Governments often make use of internal spies in accomplishing both domestic and foreign missions. Mafia, drug, and prostitution busts are obvious examples, in that those who are already within those organizations often gather much of the information that leads to such law enforcement efforts. In foreign missions, converted diplomats, generals, and city officials are sources of valuable information. *Deep Throat*, recently revealed by former FBI Associate Director Mark Felt, whose insider guidance was vital to *The Washington Post*'s groundbreaking coverage of the Watergate scandal, is an example of an internal spy used for more independent motives. News media, students, and independent investigators make use of internal spies for various projects. This can attract unwanted attention and bad public reputation.

7.3.3 Double Spies (aka "Double Agents")

Double spies, or enemy spies who have been caught and turned for the use of the organization they were originally sent to spy upon, switch for either or both of two reasons: political belief or money.

If a spy is caught and converted to a double agent, it is usually for better financial terms than he or she got from his or her previous employer. At the same time, that spy can never be fully trusted by his or her new employer.

At any time, double spies can be used as sacrificed pawns for the higher cause of the employer. This type of action has been used in many wars when converting a spy to a double agent. Double agents

are often used to transmit disinformation or to identify other agents as part of counterespionage operations. They are often very trusted by the controlling organization, because the target organization will give them true, but useless, information to pass along.

The most notorious example of a government double spy was Aldrich Ames. Ames was assigned to the CIA's Europe Division/ Counterintelligence branch, where he was responsible for directing the analysis of Soviet intelligence operations. He had access to the identities of United States sources in the KGB and Soviet military. The information Ames provided led to the compromise of at least 100 United States intelligence operations and to the execution of at least 10 United States sources. He ultimately gave the Soviet Union the names of every American agent working in the USSR.

Hackers, or those who compromise the security of computers and networks, can often be used for good purposes when caught. An example of this is Bruce Forest, who started illegally trafficking in bootleg media during the late 1980s, when the Internet was in its infancy. When his activities were uncovered, Forest was turned into a double agent and paid by Hollywood to infiltrate deep into film-sharing networks. In return, he kept his bosses informed of the techniques and activities of the pirates. He later started an independent consulting business.

7.3.4 Dead Spies

Dead spies are agents within the enemy's organization whose primary role is to spread disinformation within the organization of the opposition and to enemy spies. Double spies may also be given false information and used as dead spies.

Western intelligence agencies will often seed reputable news organizations with disinformation in the full expectation that the so-called news story will be repeated in the media. This is a modern day example of a dead spy. Dead spies can be especially dangerous in the Internet Age. They can inflict harm to an organization by spreading false information, and thus force their targets to use resources and time that they could have been spent more effectively elsewhere. Unlike living spies, dead spies disburse false information and do not actively gather it.

7.3.5 Living Spies

Living spies infiltrate an enemy and return with reports. This is the sort of typical spy that most people think of at the mention of the word *spy*.

Enemy intelligence operators are positioned for a specific situation to create maximum damage within the organizational structure of the opposition (such as returning with significant intelligence or setting up someone to spread disinformation).

Government spies are often referred to as intelligence officers. They specialize in the gathering, fusion, and analysis of information and intelligence in order to provide advice to their government. In general, intelligence officers travel to foreign countries to recruit and supervise double spies, living spies, and local spies, who in turn spy on their own governments.

A specific type of spy that is limited to the corporate realm is the labor spy. Labor spies are most typically agents hired through the services of union-busting agencies and other organizations for the purpose of monitoring, disempowering, subverting, or destroying unions, or undermining actions taken by those unions. Corporations are not subject to freedom of information requirements or sunshine laws, and corporate practices such as spying are rarely subject to public scrutiny; therefore, most information available about labor spies is historical in nature.

In the corporate world, living spies infiltrate companies and steal trade secrets. In the United States, Silicon Valley, in California, has the highest number of corporate spies. Many companies do not report corporate spies, because doing so can become a public relations nightmare and adversely affect stock prices. It can be cheaper to lose the technology than face such financial and media reactions.

During the Cold War, many Americans who traveled behind the Iron Curtain found themselves being debriefed before and after their return journey. This is an example of a non-professional living spy.

8

Social Engineering and Countermeasures

8.1 Social Engineering

Several techniques are used to penetrate physical security systems that protect sensitive information, but no matter how much technical security is used to protect this information, there still remains a vulnerability that is impossible to eliminate. As Granger (2001) states, "Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack." More directly stated, the human component of security is the weakest link and the easiest to penetrate. One of the techniques used to exploit this vulnerability is social engineering.

8.1.1 Social Engineering Defined

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is the art of manipulating people into speaking/acting contrary to their normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. They prey on human behavior, such as the desire to be helpful, the attitude to trust people, and the fear of getting in trouble. The sign of truly successful social engineers is that they receive the information without any suspicion (Damle, 2000).

In the simplest form, social engineering is "the clever manipulation of the human tendency to trust and want to help others." It is a form of deception used to access resources that would otherwise not

be accessible. The term *social engineer* has been used over the years to describe a technique that hackers use to obtain information that allows them to gain access to computer systems and files. This term is very familiar to information technology security professionals. The information that hackers try to obtain from social engineering may include the type of operating systems used, Internet protocol (IP) addresses, and passwords—information used to steal sensitive information or disrupt a company's operations.

8.1.2 Who Uses Social Engineering

Hackers may also use social engineering techniques to gain access to an organization's building and enter the network by physically being inside the building. If a hacker can gain information by social engineering, he or she reduces his or her chances of getting caught using technological methods and reduces the time it takes to gain access to a computer system or network. "Electronic attacks can be effective, but it is often easier to enter a business, sweet-talk the receptionist, and hop onto a network port in the conference room" (Higgins, 2006).

For the purpose of this study, we will not focus on the uses of social engineering for technical attacks performed by hackers. Such a topic would require a separate course altogether. Instead, this course provides information on the use of social engineering used to bypass physical security systems and gain access to facilities and nontechnical information.

Over the years, identity thieves have also used social engineering to obtain Social Security numbers, bank account numbers, and other personal information. For many years, social engineering techniques were used by criminals, foreign intelligence agents, and employees conducting corporate espionage, but they were not referred to as *social engineering*. Today, we use the term to describe any technique that deceives and takes advantage of an individual's trust for the purposes of gaining access that would otherwise not be available to the social engineer.

What type of people would use social engineering? Hackers, identity thieves, foreign intelligence operatives, organized criminals, terrorists, competitors, opportunists, and coworkers are just a few groups that use social engineering. Every piece of information gained from performing social engineering puts together a piece of the vulnerability puzzle. Social engineering is also used by security teams designed

to test the effectiveness of a physical or computer security program. Social engineers will use many techniques to obtain information that will be used to get them to the next level of access being sought.

8.1.3 Social Engineering Techniques

Some of the more common techniques social engineers use to gain information include impersonation, urgency, name-dropping, pretending to help, persuasion or intimidation, and friendliness.

8.1.3.1 Impersonation This could be impersonation of a contractor or repair person to gain entry or to justify their presence at a facility. Another means of impersonation is using fake corporate badges and posing as an employee at a smoking break area, then tailgating behind employees returning from a smoking break.

8.1.3.2 Urgency Social engineers may use the need for urgency and try to exploit someone's human tendency to want to help.

8.1.3.3 Name-Dropping Based on information gained through good research, a social engineer will use names of individuals who work in the organization to justify his or her presence within the facility or to gain information over the phone.

8.1.3.4 Pretending to Help Identifying people who require assistance and offering to help is a common tactic. An example is someone offering to help someone carrying many packages into a facility—just to gain access. Another common technique is posing as a help desk technician who is trying to solve a user's computer problem, but requires the user's log-in name and password.

8.1.3.5 Persuasion or Intimidation Using the threat of authority, the social engineer may try to intimidate an individual into providing information for the purposes of gaining access.

8.1.3.6 Friendliness This technique is used to lower an individual's guard and gain trust. A friendly person is easier to trust than someone who is not friendly.

8.1.4 Four Phases of Social Engineering

These techniques are used in combination with the Internet, telephone, mail, and personal interaction. People in the intelligence field may describe the method of personal interaction to gain information from unwitting sources as *elicitation*. There is a standard cycle that most social engineers follow to ensure successful access. We will describe the cycle in this course as the *social engineer attack cycle*. It has four phases: intelligence and information gathering, gaining trust, exploiting trust, and conducting the action/gaining access.

8.1.4.1 Intelligence and Information Gathering One of the most important phases is the intelligence and information gathering phase. Intelligence and information gathering is performed to obtain as much information as possible on the organization before any attempt to gain further access. The information obtained will be used for other phases of the attack cycle. Information can be gathered using open sources such as the library and the Internet. Another place to obtain information is through trash analysis. This is commonly referred to as *dumpster diving*. If an organization does not enforce an effective shredding policy, social engineers can gain a lot of useful information. Information obtained during this phase can provide the perpetrator a working knowledge of the organization and staff. This will enable the social engineer to seem more credible and successful when making an approach to gain trust. Staff will assume that if the individual knows that much about the company, he or she must be a valid employee. A social engineer will use professional-looking materials impersonating a business, charity, or cause. He or she will use the information obtained to develop a shallow cover story that he or she can use if questioned by anyone and to support his ploy.

8.1.4.2 Gaining Trust Once information is gathered, the perpetrator will then identify individuals to target for information. This could be the receptionist, a help desk technician, disgruntled employee, or someone who has something in common with the perpetrator. The social engineer must now make contact to gain trust (Harl, 1997). Gaining trust is a must for a social engineer to be successful. To gain trust and elicit information through personal contact, a social engineer must find locations away from the target work area to create chance encounters to

meet people. The locations can be identified through presurveillance of locations where employees socialize. Places include restaurants during lunch, smoking areas, gas stations frequented by employees on their way to or from work, and local organizations that include employees. Social engineers thrive on people being naive and unaware of the value of the information they possess and a company's lack of policies and employee education on information security. Information does not necessarily have to be sensitive or classified to be useful to a social engineer.

8.1.4.3 Exploiting Trust In certain instances, e-mail or telephone can be used to gain and exploit trust all in one phase. These methods are very successful and reduce a social engineer from unnecessary exposure and getting caught. E-mail is fabricated, printed, and used as if it were an actual e-mail sent from a valid contractor or vendor requesting information. Another method is conducting a survey, offering compensation for time and asking what appear to be valid questions.

8.1.4.4 Conducting and Action/Gaining Access The last phase of the attack cycle involves using the information gained to develop a plan and conduct an illegal act that may include stealing sensitive information, documents, or materials.

8.2 Countermeasures

Now that you understand what social engineering is, who social engineers are, and what techniques can be used, let us look at countermeasures that can be used to prevent their success.

As mentioned in the previous section, social engineering is a form of deception. There has been much research in the art of deception and how to defeat and protect against it. Lambert (1987) describes human assets for countering deception as

> " … assets in countering deception include general knowledge about and trust in well established principles about the world and events, a healthy degree of skepticism, a mind open to observing the unexpected, and a practical bent to keep one from becoming paralyzed by an overwhelming number of possibilities for deception." This is a good description of the mind-set to understand.

To reduce the threats of social engineering, a proactive approach must be taken by management. Companies must adapt to a more security-conscious culture, especially in educating employees on information security. "Social Engineering is an underestimated security risk rarely addressed in employee training programs or corporate security policies" (McDermott, 2005).

8.2.1 Training and Awareness

Social engineering training and awareness is absolutely necessary in order for an organization or individual to protect against social engineer attacks. Training is one of the most effective countermeasures. Social engineers thrive not only on people's lack of knowledge of the value of the information they possess, but also on ignorance of social engineering techniques. An organization should provide training programs to all employees including, but not limited to, security guards, receptionists, help desk employees, call centers, management, temporary employees, and vendors of the company. This training should emphasize the need for security and the various components of social engineering attacks, as well as the actions they can take to prevent unwittingly giving out information.

8.2.2 Security Measures

Along with training and education, security measures should be documented in policies and procedures to provide a guideline and to reinforce training. If an employee was asked to help someone by holding a door open because that someone claimed he forgot his employee badge—and this was clearly documented as unacceptable, the employee might remember that such a request could be a possible social engineering attempt.

A company can take these measures to avoid social engineering threats:

- Conduct a risk assessment and identify vulnerabilities and information that could be a risk to the organization if it got into the wrong hands.

- Develop information security policies that address
  - Phone security
  - Internet security (e-mail, chat rooms, blog sites)
  - Badge and access control card policies
  - Document handling
- Conduct in-depth and recurring education on social engineering and information security.
- Shred all documents—whether classified or not.
- Screen information that is on the company's Internet website and information released in news releases and marketing materials.
- Publish only a single phone number as contact for the company, and have all calls transferred from that number to the appropriate contact.
- Develop a clean desk policy—do not leave documents on your desk when you leave for lunch and at end of the day.
- Reduce access to critical and sensitive information.
- Do not reveal personal or financial information in e-mail, and do not respond to e-mail solicitations requesting this information. This includes following links sent by e-mail.
- Install and maintain firewalls, antivirus software, antispyware software, and e-mail filters.
- Limit the ability of employees to copy information on the network; disable recordable CD drives, USB ports, and floppy drives, except for certain positions.
- Conduct background checks on all people in positions that handle sensitive information, including contractors and vendors.

Bibliography

Granger, S. (2001). Social engineering fundamentals. *Part I: Hacker Tactics*.

Lambert, D.R. (1987, October). Technical report 1076. "A cognitive model for exposition of human deception and counterdeception." Retrieved from http://www.unhca.com/NSP/Decep.html.

McDermott, J. (2005, September 7). *Social Engineering the Weakest Link in Information Security*. Windows Network Security Library. Retrieved from http://www.windowssecurity.com.

9
Deception Detection

9.1 Establish a Baseline

When is the best time to recognize that an employee is being deceptive? The answer is during the interview, before a hiring decision is made.

When people are asked how a person can tell when someone is lying, studies have shown the most common response is that liars avert their gaze. "This is … the most prevalent stereotype about deception in the world," says Charles Bond of Texas Christian University. While gaze aversion is a statistically reliable indicator of deception, it has not been proven as the indicator with the highest correlation to lying. Indicators commonly held as reliable are discussed in this section.

However, even these signs are often questioned, as each individual exudes different characteristics when lying and when telling the truth. An emphasis lies in comparing all actions to the baseline behavior. To establish the baseline, the interviewer should ask noninvasive questions—questions with simple answers, questions to make the person being interviewed feel more comfortable. While the interviewer asks these baseline questions, he or she should be aware of the subject's eye contact, voice, body language, and facial expressions. If the interviewer is able to establish how the person behaves when telling the truth, there is a greater possibility of recognizing a departure from this normal state, which could be a lie.

9.2 Common Suspicious Behaviors

9.2.1 Eye Contact

On average, a person will make eye contact for at least half of a conversation. If someone avoids eye contact or constantly looks down

during a specific part of a conversation, it could be an indication of a lie. Typically, people will not look directly into the eyes of a person to whom they are lying. However, because this is such a common behavior of lying, good liars are aware of this perception. Thus, they will go to great efforts to make and keep eye contact when lying.

Breaking eye contact can actually be a signal of information retrieval, usually signifying truth. Generally, when an individual attempts to recall visual information, their eyes will move up. This is how they retrieve mental pictures. So lying individuals could keep eye contact because they do not need to retrieve information from their mind; they have already developed a story to tell. Another indication of lying eyes is a lack of blinking.

9.2.2 Change in Voice

A variation in the pitch of a person's tone or the rate of speech, as well as a lot of stammering (*uh*, *um*, *ah*) or throat clearing could indicate a lie.

Also, liars will often talk too much and provide more information than requested. This is an attempt to cover up lies. By befriending the interviewer, they think they can get the interviewer on their side. On the other hand, be aware of unpleasantness. "Liars are noticeably less cooperative than truth-tellers," found psychologists Bella M. DePaulo and Wendy L. Morris in a review of studies on deception. "Liars also make more negative statements and complaints than truth-tellers do, and they appear somewhat less friendly and pleasant," continue DePaulo and Morris.

The liar might also protest too much—someone who consciously is trying to make you think he or she is honest may be lying. Why would they assume you think they are lying? Maybe because they are!

9.2.3 Body Language

When an individual lies, he or she attempts to draw attention away from the lies being told. This diversion tactic is often witnessed in body language. Liars will often touch their nose, mouth, chin, or hair—by putting a hand in front of the mouth, it is as if they are hiding the lies. They might turn away or fidget with their hands or legs.

Sweating can also be a key indication. Nervousness can also play a part in these physical clues.

People who are lying will often cross their arms in front of the body, in a sense protecting themselves. This is a signal of withdrawing from reality. Liars might also have a difficulty standing still, so it is common for them to shift weight from side to side or pace around the room. For this reason, it is best to have the subject sit down when attempting to draw out the truth.

9.2.4 A Mixed Signal

When someone is lying, you can typically find inconsistencies in various forms. First is the obvious inconsistency in facts. Statements that just do not hold together should make the interviewer suspicious. Ask the subject to repeat his or her story and listen for inconsistencies to hunt out lies.

Next, look for inconsistencies in the words a person says versus the facial expression held at the time of the statement. When a person is telling the truth, the two match. For example, if a person honestly says he or she likes you, her face is relaxed, as he or she offers a kind smile and gently eyes. But when he or she is lying, he or she may not be smiling, or he or she might even have a clenched fist. These physical clues do not match the words spoken. It is a mixed signal—look for these mismatches between words and body language.

9.3 Macro and Micro Expressions

The above characteristics are statistically accurate in detecting lies, but a good liar could easily conquer them. Dr. Paul Ekman, a retired psychologist from the University of California, San Francisco, is famous for his research on reading subtle emotional cues from the face, voice, and body language of an individual. Dr. Ekman developed a research tool called Facial Action Coding System (FACS) for deciphering which of the 43 muscles in the face are working at any given moment. This tool can be used even when an emotion is so fleeting that the person experiencing it may not be conscious of it. These are called *micro expressions*. Those that a person is conscious of are called *macro expressions*.

Experienced liars are able to alter voluntary facial expressions and body language to appear in harmony with their words (the liar has conquered the mixed signal). Interviewers often note the harmony of all indicators, and thus are deceived. However, by looking at micro expressions, an interviewer can detect the lie. According to Ekman, deception will almost always show up in the face as an inconsistency between the micro and macro expressions.

Ekman defined micro and macro patterns as follows.

9.3.1 Macro Expressions

General behaviors:

- Increased discomfort/anxiety
- Hostility
- Unmerited anger toward you
- Persistent evasiveness/resistance

Posture:

- Extreme rigidity followed by alternating stiffness and relaxation
- Hands, legs, or objects put in front of body to form a barrier
- Feigned lack of interest
- Posture changes caused by topic changes
- Not facing you
- Distancing or leaning away

Gestures and movements:

- Rubbing the forehead near the temple region
- Squeezing the face
- Rubbing the neck
- Stroking the back of the head with the hand
- Using fewer hand movements to illustrate actions than usual
- Movement away from you
- Lip-licking
- Hard-swallowing
- Wringing hands
- Hiding the eyes

9.3.2 Micro Expressions

General expressions:

- Averting the eyes
- Focusing the eyes
- Face whitening
- Face flushing

9.4 Eye-Accessing Cues

By the direction of where the person's eyes are looking, you can determine whether they are using vision, sound, or kinesthetic (feeling) to trigger their thinking:

- Up and to the left (your upper right)—They are accessing visual memory.
- Up and to the right (your upper left)—They are visually constructing or imaging something.
- To the left (your right)—They are remembering a sound.
- To the right (your left)—They are creating a sound.
- Down and to the right (your lower left)—They are accessing a bodily feeling or emotion.
- Down and to the left (your lower right)—They are accessing inner dialogue (talking to themselves).

Keep in mind that this is reversed for left-handed individuals.

9.5 Truth Detection Equipment

9.5.1 How Traditional Truth Detectors Work

Polygraphs have been around since 1921, when John Larson, a California medical student, invented a machine that measured physiological changes that occur because of the stress many people feel when they tell a lie (Bellis, 2007).

The lie detector works by applying four to six sensors to the test subject and measuring such factors as sweating, blood pressure, breathing rate, and pulse. More advanced polygraphs will also combine voice stress measurements, and may measure such things

as leg movements (HowStuffWorks, 1998–2007). During the test, a questioner will set a baseline by reading a series of questions—asking the subject to tell the truth on some and to lie on others. Answers to pertinent questions are then compared to the baseline. In the hands of an effective examiner, the polygraph tests have had a good record of accuracy. However, the interpretation of the results is subjective.

A subject can fool a polygraph test in many ways, especially if the subject has exceptional control over his or her responses. Some may employ distraction techniques to help them to either raise stress levels during truth telling or lower stress levels as they tell lies.

9.5.2 1988 Employee Polygraph Protection Act (EPPA)

Other technologies, such as voice stress detectors, do not require the use of sensors. However, this technology is regulated along with polygraph tests by the 1988 EPPA. Privacy advocates have challenged the widespread use of polygraph testing because of a perceived invasion of employee privacy. Their lobbying efforts led to the passage of the act, which prohibits most private employers from using lie detector tests either for preemployment screening or during the course of employment. The law prohibits employers from requiring employees to submit to lie detector tests in most situations, including interviewing, discipline, or termination (United States Department of Labor, Employment Standards Administration Wage and Hour Division, 2007).

There are some exceptions to the act—most notably, the act does not apply to federal, state, or local government employees. It also does not apply to security service businesses hiring security-intensive positions, such as a driver of an armored car. It also does not apply to pharmaceutical manufacturers. The government in 1995 expanded the act to apply to some federal employees. So any government agency should seek guidance before using polygraph technology (United States Department of Labor, 2007). A business may require a polygraph test for an employee who is the subject of an investigation of an incident that caused specific economic loss or injury to the employer.

9.5.3 Legal Requirements

Where polygraph examinations are allowed, they are subject to strict standards for the conduct of the test, including the pretest, testing, and post-testing phases. An examiner must be licensed and bonded or have professional liability coverage. The act strictly limits the disclosure of information obtained during a polygraph test (United States Department of Labor, 2007).

The advice for government entities and private businesses is to be careful not to violate the law when considering whether to require a polygraph test. It would be wise to consult with a lawyer or to get clarification from the Employment Standards Administration Wage and Hour Division before requiring a test.

For a deeper understanding of the Employee Polygraph Protection Act, see the full legislation, printed in the Appendix.

9.6 Your Intuition

Finally, one of the most important factors in detecting a liar is good old-fashioned intuition. Often lies will provoke feelings of uncertainty—that something is just not right with a story. Do not ignore your intuition. Dig deeper.

On the other hand, beware of your intuition when it tells you that someone would not lie because he or she is just not that kind of a person. History proves time and again that just about any type of person can become a liar under the right circumstances. Again, distrust your judgment of character. There is no one you know completely—probably not even yourself. There is simply no way of judging another person's reactions and motivations with 100 percent accuracy. So the best advice is to go with your intuition when it advises caution and prudent wariness. Distrust your intuition when it steers you toward blind trust.

9.7 Handwriting Analysis

Handwriting analysis or graphology is also a tool to detect deception, and like the polygraph, it is controversial. It is being used increasingly by businesses, partially in response to prohibitions on using polygraph testing (Washington University Law Quarterly, 1997).

Graphology is not to be confused with forensic document examination, which is often used to compare samples of handwriting to determine whether they are from the same subject or are forgeries. Graphologists believe that personality traits can be ascertained by many aspects of handwriting. However, like polygraph testing results, this type of handwriting analysis is not usually allowed in court proceedings.

Problems that have been cited with handwriting analysis include the differences of opinion that exist among handwriting analysts, and the subjective nature of the study. Like polygraph testing, the success that graphology can achieve often relies on the person doing the analysis.

Legal problems may ensnare employers who are seen as abusing the use of graphology. According to an article in the Washington University Law Quarterly, an employee may sue based on any of these grounds:

- Defamation
- Discrimination
- Violation of the Americans with Disabilities Act
- State antidiscrimination laws
- Invasion of privacy

Many employee advocacy groups, including the American Civil Liberties Union, denounce graphology as *pseudoscience* which unfairly discriminates against people based only on how they write.

There is no denying, however, that a skilled graphologist can make uncanny observations about the personality of a writer. Criminal profilers working to solve challenging cases have often used this skill.

PART III
Personal Information Security

CHAPTER 10 Home Computer Security
CHAPTER 11 Security while Traveling

10
Home Computer Security

Keeping your identity and personal information private, while still using the Internet as a communication and business tool, can be a confusing and daunting undertaking. Identity theft, malicious codes (viruses), and file confidentiality are all issues the average person confronts daily.

10.1 E-Mail Issues

According to a study from the first quarter of 2006, there are about 1.1 billion e-mail users worldwide, and approximately 171 billion e-mails are sent daily (or about two million e-mails every second). Approximately 70% to 72% of these e-mails are estimated to be spam or viruses. These numbers are expected to be increasing. Clearly, people should examine their e-mail security and processes as a first step in protecting themselves online. Basic security steps to protect e-mail integrity should include changing passwords monthly, creating secure pass phrases, and logging out of web-based e-mail after use.

10.1.1 Passwords

To create a secure pass phrase, follow these guidelines:

- Do not use personal information in a password. This includes your pet's name, child's name, birthday, and other information. It is easy to guess! Example: Susan 1979
- Do not use real words. This is more difficult for most people to avoid, because it makes remembering passwords easier. But for the most secure passwords, you should not use real words because computer scripts do not take much time to go through every word in the dictionary. Example: Security

- Use different characters and character types. Use uppercase, lowercase, and numbers in your password. Make use of special characters such as *&^ if your program or provider allows for them. In other words, use the top of the keyboard and the Shift key. This is along the lines of a pass phrase for ease of memory recall. Example: &ecurity-0f-our$h0me (security of our home)

How do you remember your new, secure passwords? Try using simple mnemonics to create and remember. *Mary had One little Silly lamb in 73* could be converted into a password like *Mh0l$Li73*. By substituting the *0* for *O* and *$* for *S*, this password is much harder to crack, but still easy to remember (if the application does not allow special characters, go ahead and use *S*). If you are still afraid of forgetting your passwords, write them on a piece of paper and put that paper in a locked safe with your other important documents.

10.1.2 Corresponding Online

When corresponding with financial institutions and other businesses online, including PayPal, it is most secure to initiate *each* contact. This means ignoring all unsolicited e-mail (this cannot be stressed enough: The New York State Consumer Protection Board recently found that e-mails claiming to be fraud alerts are the newest wave of identity theft scam). Often, there are codes written into the e-mail that will either direct you to a fake site and steal your information (phishing and spoofing) or record information you enter on the genuine site. A more secure way to go about corresponding with your bank (or other institution that has access to or where you might enter your personal information) would be to

1. Clear your browser cache.
2. Type in the institution's web address (e.g., HSBC.com, Amazon.com).
3. Log into your account and navigate to where you contact customer service or help.
4. When your bank or institution responds, if it is from an e-mail address, do *not* respond and send personal information (the bank or institution should already have it). Keep the

questions and answers specific to your particular issue. If you must give out personal information, repeat steps 1–3 again and note that you have been in correspondence with someone already.

By setting secure pass phrases, ignoring *all* unsolicited e-mail claiming to be from businesses, and by securely instigating communication with institutions, most problems related to e-mail security will be prevented.

10.1.3 Mail Bombs

A common e-mail annoyance, although not necessarily a security issue, is the mail bomb. A mail bomb is the delivery of enough e-mail to a mailbox to overload the mailbox or perhaps even the system that hosts the mailbox.

Mail bombs generally take one of two forms. A mailbox might be targeted to receive hundreds or thousands of messages; this makes it difficult or impossible for the victim to use the mailbox, possibly subjects him or her to additional charges for storage space, and might cause the victim to miss messages entirely because of overflow. This is seen as a denial-of-service attack, perhaps also harassment, and is not tolerated by any known service provider.

Alternatively, a message can be bulk e-mailed, with the intended victim's address forged in the *From:* and/or *Reply-To:* lines of the headers. The victim is then deluged with responses, mostly angry.

There is a third, particularly nasty, form of mail bomb. This one forges subscription requests to many mailing lists, all for one recipient. The result is a huge barrage of e-mail arriving in the victim's e-mail box, all of it unwanted, but legitimate. Many mailing list administrators are countering this form of abuse by sending a confirmation e-mail to each subscription request, which must be returned in order to be subscribed to the list" (The e-mail abuse FAQ, 2006).

Contact your Internet service provider (ISP) immediately! They can often find the source of the mail bomb and can take steps to stop it. To prevent being mail bombed, do not fill out e-mail forms; do not use your real e-mail address on forums, websites, and message boards; or have a separate e-mail address for these uses.

10.2 Website/E-Commerce Issues

When making purchases and conducting business online, it can be difficult to discern which merchants to trust. Consider the following data from the 2006 Internet Crime Report:

- Internet auction fraud was by far the most reported offense, comprising 44.9% of referred complaints. Nondelivered merchandise or nonpayment accounted for 19% of complaints.
- Of those individuals who reported a dollar loss, the highest median losses were found among Nigerian letter fraud ($5100), check fraud ($3744), and other investment fraud ($2695) complainants.
- E-mail (73.9%) and web pages (36.0%) were the two primary mechanisms by which the fraudulent contact took place.

In order to prevent auction fraud, one should understand Internet auctions as much as possible, learn what actions the auction website takes in case there are problems, learn as much as possible about the seller (start with Google or other search engine searches with information in quotation marks; sellers will not always be listed with the Better Business Bureau, but it is a good idea to check anyway), and use caution when paying—especially if the seller is requesting check or money order sent to a PO box. Obtain warranty/exchange/shipping information, and *never* give out your Social Security or driver's license number (sellers have no legitimate use for this information).

There are also common sense tips for preventing credit card fraud online. The FBI recommends investigating companies thoroughly before doing business with them. Some often overlooked methods of company investigation include the following:

- Attempt to obtain a physical address and phone number, rather than a PO box. Call the seller to see if the number is correct and working.
- Be wary of sellers who use free e-mail services such as Hotmail, Gmail, Yahoo, and other services that do not require a credit card to open an account. An example of a better e-mail address

would be something like *fred@fred.com*—domain names and web hosting providers charge for service and, therefore, a credit card was used and the business is thus more traceable.

- Always make online purchases with credit cards, because often you can dispute the charges if something goes wrong. For extra protection, obtain and use one credit card (even better is a prepaid card such as those offered by Western Union) specifically and *only* for online purchases. This will make your purchases traceable and organized.

10.3 Social Networking and Cyberstalking

With the rise of Internet usage and its increasing use as a social and community tool, it is important to prevent becoming a victim of cyberstalkers when conducting normal online activities (such as creating online profiles on sites such as MySpace, YouTube, and other interactive social sites). Cyberstalking is the use of the Internet to harass, threaten, follow the activities of, and otherwise stalk someone. As with non-Internet stalking, women are most often victims and men are most often perpetrators.

Some tips on preventing becoming a victim of cyberstalking and harassment include the following:

- Use gender-neutral usernames and e-mail addresses.
- Use free e-mail accounts (Yahoo, Hotmail, etc.) for newsgroups, forums, chat rooms, social networking, blogging, and other online activities where you might come into contact with strangers.
- Do not write things in forums that you would not feel comfortable saying to someone's face or in front of a group.
- Avoid revealing personal details such as your specific neighborhood, last name, and employer. If you live in a small town, you might consider naming the nearest larger city as your residence.
- Consider getting a free temporary call forwarding number through a site such as craigsnumber.com or an easily changeable (and forwardable) voice-over-IP number from a company such as vbuzzer.com.

- Be careful of posting pictures. Consider using an image-editing program to clearly watermark images with your public e-mail address or username. This will make it much less likely to be stolen and used on other sites. Also, beware when e-mailing and posting pictures that you would not show to your company management. If you feel inclined to post or send potentially embarrassing pictures, edit them so that your face is not clear and be careful that there are no license plates or other potentially identifying information discernible!

When it comes to interacting with others and revealing information, two good questions to ask yourself are "do they need to know this?" and "how would I feel if my work management found out about this picture/comment/blog/expression?" Finally, use your common sense and your gut feeling.

Go to http://www.haltabuse.org for more information on cyberstalking and harassment.

10.4 Other Issues

Laptop theft and other forms of off-line identity theft are more common than online crimes, the Javelin Identity Fraud Survey Report found. Will the loss or theft of information on your laptop endanger your vital personal and financial data? Besides the data stored on your hard drive, there is that which is in your files within Quicken, Word, Excel, e-mail correspondences (especially if you download from a program such as Outlook or Thunderbird), stored usernames/passwords, personal photos, and much more!

The first solution to avoid experiencing a damaging theft is obvious: do not store any data on your laptop that could be damaging if lost. If you must store such information on your laptop, recommends ConsumerAffairs.com, put it in a subdirectory on your computer so that when you travel it can easily be removed to a more secure situation (memory stick or your desktop computer disk).

Hard-drive encryption is another tool to prevent the theft of sensitive information from your laptop. Do a search for *hard-drive encryption software* and make an informed decision after researching

different software options. A good place to start is download.com (by CNet), under the category *Security and Spyware*. However, be sure to remember that "any computer that contains encrypted information is self-contained and, as such, everything that is needed to decrypt the information is also present on that computer" (Cole, 2007).

To keep your laptop physically secure, consider making a habit of taking these precautions: never leave it in your car, always lock it with a security cable when not in use, never leave it alone (not even at your local coffee shop), keep it off the floor or at least between your feet, be vigilant in hotels by locking it in the fire safe, and be aware of nosey people who might be looking over your back when you are entering in sensitive passwords (best idea: do not access banking sites when out in public!).

Storage devices, such as flash cards, USB drives, DVDs, and other removable devices can also be sources of data theft. Label all units clearly, encrypt them, and store them in a padlocked fire safe when not in use. Consider limiting the number of removable devices used on a daily basis. If you use only one flash card, for instance, this will make data much easier to track.

When it comes to deleting files, it is recommended to use special software for complete deletion—emptying your recycle bin does not permanently remove files! As with hard-drive encryption, you should research different software and obtain it only from reputable sources. When disposing of your computer, the most secure way to delete files is to destroy the hard drive by submerging it in hot water. If you are donating or selling your personal computer, be sure to remove *only* the hard drive (other parts of the computer do not store data and are usable). Buying a new hard drive or two is considerably less expensive than dealing with the effects of data theft!

Finally, consider that half of all identity fraud is committed by someone the victim knows (family member, friend, employee, neighbor, etc.). Have different usernames and passwords on your computer if different family members are using it. Set permissions so that only the *admin* can access files and use programs that might compromise financial and personal security. Set your computer to require re-entering the username/password after 5 minutes (or less) of inactivity. Create secure passwords and change them often.

By using common sense, making use security technologies, and by taking preventative actions, you will be far less likely to end up as one of the approximately 10 million victims of identity fraud, nor in the countless numbers of those who have had sensitive data stolen.

Bibliography

Cole, E. (2007, April 10). *The Secrets of Laptop Encryption*. eSecurityPlanet. Retrieved July 26, 2007, from http://www.esecurityplanet.com/views/article.php/3670566.

How many e-mail users are there? Retrieved July 26, 2007, from http://e-mail.about.com/od/e-mailtrivia/f/how_many_e-mail.htm.

How to clear cache in Internet Explorer. Retrieved July 26, 2007, from http://www.1line.williams.com/webbi/html/ClearCacheIE.html.

Huffman, M. (2007, March 5). *Phishing Scam Takes New Tack*. Consumer Affairs. Retrieved July 26, 2007, from http://www.consumeraffairs.com/news04/2007/03/phishing_tactic.html.

Identity theft/data security news. Index of Most Current Stories. Retrieved July 26, 2007, from http://www.consumeraffairs.com/news_index/id_theft.html.

Identity theft more prevalent offline, report finds. Retrieved January 31, 2006, from http://www.consumeraffairs.com/news04/2006/01/id_theft_survey.html.

Laptop security. Retrieved June 2007, from http://onguardonline.gov/laptop.html.

StatiX. SxSecurity. Retrieved June 5, 2007, from http://www.sxsecurity.com/Privacy/Destroy_Your_PC_before_trashing_it/.

The e-mail abuse FAQ. (2006). Retrieved July 26, 2007, from http://members.aol.com/e-mailfaq/e-mailfaq.html.

The Internet Crime Complaint Center. 2006 Internet Fraud Crime Report: January 1, 2006–December 31, 2006. Executive Summary. Retrieved July 26, 2007, from http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

11

Security while Traveling

One area deeply impacted by SSI, especially since 9/11, is the transportation industry. Each year, hundreds of thousands of United States citizens travel for either business or pleasure. For most people, traveling is a positive and rewarding experience. For the few who experience security- or safety-related problems, a lack of planning and general awareness are often contributing factors. Whether you are an experienced or first-time traveler, you should take your personal safety and security seriously. Thus, issues of SSI while traveling should not be a concern.

Good security habits will not detract from your travel but will instead serve to enhance it. The following information is provided to help individuals avoid pitfalls while traveling and provides security reminders to assist individuals in planning for their trip. Protecting your own SSI is important, especially during foreign travel.

11.1 Travel Preparations

The preparations you make before you depart for your trip will depend on the destination, length, and purpose of your trip. Before leaving, be sure to confirm lodging and travel reservations and obtain traveler's checks. Unless anonymity is an issue, also leave a copy of your itinerary with a relative or close friend. You should take with you pertinent information regarding health insurance coverage that might be useful in an emergency. Also, if you are traveling on business, you will need any official documents, and some overseas destinations require vaccination information. These suggestions will help you prepare for your trip:

- Learn about the places you plan to visit. Familiarize yourself with local laws and, if traveling overseas, customs in those areas you will be visiting. Information can be obtained from

your public library, local travel agency, or the United States State Department.

- Leave behind any government identification (badges, security passes, phone numbers, etc.) that is not necessary in your trip. If it is necessary, hide it in a secure place in your carry-on luggage. Leave behind photographs of family members and loved ones, which could be used as coercion by terrorists and criminals.
- Ensure that you are equipped with all official documents (passport, shot records, official orders, etc.).
- Grant power of attorney to an immediate relative or close friend. Complete or update your will to include naming a guardian for any minor children.
- Establish a point of contact for your family to call in an emergency.
- Carry an extra set of eyeglasses and any necessary medications, along with copy of the prescription and/or generic name of the drug, in your carry-on luggage.
- Keep all medications in their original containers.

11.2 Importance of Identification

Make copies of your airline ticket, itinerary, passport identification or bio-page only in black and white, driver's license, and credit cards you are taking with you (it is recommended that you take at least two credit cards). Make another copy for your immediate family or a close friend who is not traveling with you. Carry two extra passport photographs in a separate place from the originals. These items will help speed the replacement process should the documents be lost or stolen.

Take all essential personal and medical information you will need to get you through your trip successfully. Do not travel with your birth certificate. The passport is the best document for traveling in and out of another country. Alien smugglers could use a birth certificate to steal your identity and assign it to another person.

Never leave your wallet or purse unattended. Carry your information on your person at all times.

11.3 Travel Precautions

11.3.1 Destination Arrival

To ensure the safety of your important information when traveling by plane, follow these tips:

- Once you have landed, proceed directly to the baggage claim and customs areas. Keep a low profile. If you are traveling abroad, be courteous and cooperative when processing through customs.
- Stay alert, check out emergency exits, and keep your distance from unattended luggage.
- Do not leave your own belongings unattended.
- Never agree to carry a package for a stranger for any reason.
- Report unattended luggage to airport security personnel.
- Exit the airport as quickly as possible.

11.3.2 Rental Vehicles

To ensure the safety of your important information in vehicles, follow these tips:

- Always drive with the doors locked and windows closed.
- Be cautious of anything that causes you to make an abnormal stop.
- Never pick up hitchhikers, and if you observe an accident, drive to the nearest telephone or police station to report it.
- Always lock your car when you leave it unattended and avoid leaving valuables in the car even if locked in the glove box or trunk.
- Inspect your vehicle for tampering inside and out. If you suspect a problem, keep clear of the vehicle and contact the authorities.

11.3.3 Hotel

To protect your important information in a hotel, follow these tips:

- Avoid taking a street-level room. Choose a room between the second and seventh floors: too high for easy outside access and low enough to be reached by fire equipment.
- Use elevators rather than stairwells. Stand near the control panel so if threatened you can push the alarm button.
- Report lost keys immediately and consider changing rooms.
- When in the hotel room, secure the door and windows and keep them locked. When you leave your room, do not leave indicators showing that you are out. In fact, leave the television or radio on, giving the impression that the room is occupied. Do not leave anything of value (money, tickets, camera, etc.) or work-related items (briefcases, computers, etc.) in your room when you go out, even if locked in your suitcase.
- Do not accept deliveries to your room unless previously arranged and you are certain of the source and contents.
- Keep your room key with you instead of leaving it at the front desk.

11.3.4 Personal

- Always be conscious of your surroundings and avoid any areas you think may put your personal safety at risk.
- Be especially careful not to flash large sums of money. It is also best to leave your valuables (anything of high monetary or sentimental value that you cannot afford to lose or will be unable to replace) such as jewelry or expensive luggage at home.
- Avoid high-crime areas and never travel alone after dark.
- When traveling on foot, walk only on well-lit, heavily traveled streets when possible.
- Avoid shortcuts through alleys or side streets. Walk in the middle of the sidewalk and secure your belongings.
- Be wary of street vendors and innocent-looking youngsters. While one person has your attention, someone else may be picking your pocket.
- Should a suspicious-looking person approach you on foot, cross the street or change direction. If the occupants of a car threaten you, move in the opposite direction.

- Remain alert, and if you have a problem, go to the local police department.

11.4 Precautions while Staying in a Foreign Country

If your destination is a foreign country, the tips that follow will assist you in having an enjoyable vacation or productive business trip.

11.4.1 Protect Your Passport

Your passport is the most significant identification you will carry. This is your proof of United States citizenship while traveling abroad. Passport theft, particularly of American tourist passports, is on the increase. Take extra precautions to protect your passport because its loss or theft may cause you unnecessary travel complications as well as significant expense.

- To minimize potential loss or theft, it is recommended that you carry your passport in your front pants pocket or in a pouch hidden in your clothes.
- Do not leave your passport at the hotel's front desk—an employee could scan the document to commit identity fraud. Some areas use this procedure to register you with the local police as a routine policy. Do not forget to ask for a receipt and be sure to retrieve your passport before continuing your trip.
- Use discretion in displaying your passport, as it could draw undue attention to you. Memorizing your passport number and other essential information will help you avoid flashing your passport around when filling out items such as landing cards and hotel registration forms.

If your passport is lost or stolen abroad, report the situation immediately to the nearest United States Embassy or Consulate and to the local police authorities. Again, having copies of your passport bio-page, along with extra passport photos, will help speed the replacement process.

11.4.2 Safeguard Your Laptop Computer

You should never leave your laptop computer unattended, especially when traveling overseas. Foreign governments are hungry for United

States information of any type. Many foreign countries do not have the same laws as the United States regarding privacy and freedom from unreasonable searches. If you leave your computer unsecured for a day in your hotel room, assume that the files on it have been copied. If your computer is stolen and returned to you within the day, or within a few days after traveling on a train or staying in a hotel, assume that the files have been copied. In order to minimize the risk of this happening, you can either keep your computer in a safety deposit box at the hotel or keep it with you at all times. Do not put it down or leave it unattended for any length of time.

11.4.3 Establish Points of Contact

Establishing points of contact is important. Someone should know your whereabouts from the time you depart the United States until you return home. Provide your contact with a detailed copy of your itinerary and advise him/her of any changes. If you are traveling on business, you should establish a point of contact in the country you are visiting. Be sure to carry that person's name and telephone number with you.

Depending on your personal circumstances or if your travel involves an extended stay, it may be advisable to register with the nearest United States Embassy or Consulate. This will make it easier should someone at home need to locate you urgently or in the unlikely event that you need to be evacuated due to an emergency.

11.4.4 Keep a Low Profile

You need to use common sense and be extra conscious of your appearance and actions so that you do not attract unwanted attention. Take a good look at the items you plan to take with you such as clothing, jewelry, and even religious items. This is especially true for reading materials that may be considered offensive. Keep in mind that certain items may not be appropriate in the country you are visiting. Have a brief read about the foreign country that you are going to visit.

Avoid clothing and other outward vestiges that unnecessarily advertise you as an American citizen. Wear nondescript, casual apparel that

enables you to blend in as much as possible. Leave behind professional sports apparel items, hats, coats, shirts, and western apparel.

11.4.5 Shun Publicity

Shun publicity and inquiries by the local news media. If approached by the media, remember not to disclose any information relating to yourself or other government personnel and to report such contacts to your agency or supervisor.

Avoid discussing personal and background information concerning yourself and family members with nationals of the country you are visiting.

11.4.6 Local Laws

Although you are an American citizen, you are subject to the laws of the country in which you are traveling. Do not assume that acceptable behavior in the United States is acceptable abroad. For example, in many countries individuals are prohibited from making derogatory comments about the government or government leaders. Taking photographs of government facilities and religious symbols is also prohibited in many countries. Therefore, be aware of the local laws. As a general rule, do not attempt to take photographs in the vicinity of foreign military bases, buildings, or personnel.

11.4.7 Money Matters

- Take most of your money in international traveler's checks. Do not carry large amounts of cash.
- Plan ahead to ensure that you will have enough foreign currency for the expenses you anticipate during your first day in the country. It is advisable to exchange some money to cover such essentials as taxi fares, meals, and tips.
- Do not rely on currency exchanges at airports being open 24 hours a day. Local banks usually offer the best rates, although hotel money exchanges may be more convenient.

- Always deal with reputable established currency exchanges—in many countries it is illegal to do otherwise. If you deal with people on the street who offer you an unbelievable deal, you run the risk of getting counterfeit currency or being arrested for involvement in black market activity.
- Be sure to keep track of all your transactions. Each time you cash a traveler's check, record the serial number, denomination, date, and location of purchase. Keep this in a separate place so replacement checks can be issued quickly if they are lost or stolen.
- Safeguard the credit cards as well as customer copies of each credit card transaction you make. Any credit cards that are unnecessary or invalid overseas (e.g., gasoline or department credit cards) should be left behind.

11.4.8 Medical Problems and Emergencies

- To help prevent illness while you are abroad, get a medical checkup before your trip and make sure that your immunizations are up to date.
- Do not hesitate to seek medical assistance if you need it. Should you require medical services because of injury or serious illness, contact the nearest United States Embassy or Consulate, where a representative is on duty 24 hours a day. This individual can provide the names of reputable physicians and hospitals who can help you avoid improper treatment and/or medical bills. In most cases, hotel personnel also provide good advice, although there have been reports of clerks who have arrangements with unethical physicians.

11.4.9 Arrest

If you are arrested for any reason, ask permission to notify the nearest United States Embassy or Consulate. In some countries, your request may not be honored immediately. *Be persistent.*

A consular officer cannot arrange for free legal aid or provide bail money for you. The consular official can only provide you names of

English-speaking attorneys and help you find adequate legal representation. He or she can contact your traveling companions or relatives in the United States, or intervene if you are receiving discriminatory treatment.

11.4.10 Illness or Medical Emergency

- Carry a summary of your medical history, including past illnesses, allergies, and blood type.
- Carry an ample supply of any prescription medication you are required to take. It is also recommended that you take along an extra prescription in case you need a refill. Be sure to ask for the generic name of any prescription drug because brand names differ in other countries.
- Always leave medicines in the original labeled containers.
- Check with your medical insurance agent to make sure your medical expenses will be covered if you incur an injury or illness while traveling.
- If you need information about diseases, shots needed, etc., contact the Centers for Disease Control and Prevention at (404) 332-4559.
- If you need information for English-speaking doctors in foreign countries, contact the International Association for Medical Assistance to Travelers at (716) 754-4883.

PART IV
SECURITY WITHIN BUSINESSES

CHAPTER 12 Securing Business SSI
CHAPTER 13 ANSI Standards
CHAPTER 14 Corporate National Institute of Standards and Technology (NIST)
CHAPTER 15 Cybersecurity

12
Securing Business SSI

12.1 Corporate Spying

Abbott Laboratories, like most pharmaceutical firms, did everything it could to protect its plant from falling victim to corporate spying. The company installed timers on its gates so they would only open for short periods during shift changes, work areas were isolated and guarded, and employees did not bring anything in or out of the office without it first being carefully scrutinized. Despite these precautions, Abbott brought suit against two employees for duplicating the company's formula for an artificial sweetener. How did the employees get past the safety measures that Abbott had taken? They memorized the formula. This is not a story of a recent episode of corporate spying—it happened in March 1965. And corporate spying is even more prevalent today.

12.1.1 Spy Techniques/Technology

Times have changed since 1965. Technology being what it is today, corporate spying and theft is easier than it has ever been. Spies can gather information regarding the target company just by knowing what they are looking for on the Internet and how to access it. A few friendly phone calls to the company can open up doors to information as well—not to mention posing as an employee or as someone who may have an interest in the company. Cell phones and personal digital assistants can be synched with work computers, jump drives are easy to come by, and many companies are allowing their employees to work from home, meaning that confidential information may not be confined to just the office anymore. These variables make it easy for someone to walk away with client lists, intellectual property, company

bylaws, and other confidential information vital to the success of a company.

In 1997, the world of frozen pizza was about to be turned upside down. Rumors had been rampant that Kraft was preparing to roll out its latest product: the DiGiorno rising crust pizza. Schwan's had figured out the secret to the rising crust and was also preparing to release its own rising crust brand, Freschetta—however, the company was not sure how long it had to perfect it before the DiGiorno pizzas hit the market. Schwan's knew that the success of its product relied on information they did not have. Schwan's executives knew that, technically, the information could be legally obtained through publicly available sources because the Economic Espionage Act of 1996 only protects trade secret information, but feared the amount of time it would take. Enter Marc Barry. Barry is a consultant hired by corporations when they need someone to gather information, but do not want to be held accountable if some unethical measures are taken. In industry terms the person is known as a *kite*—someone the company will cut loose claiming that he or she did not know the methods in use, giving the company plausible deniability.

Barry began by doing some basic research, set up voice-mail and fax machine numbers that would be local to the area the Kraft warehouse was located and started making phone calls. He posed as a reporter, an environmentalist, a businessman, and a graduate student when calling everyone from government officials to a Kraft loading dock employee. In doing so, he was able to gather all of the information Schwan's needed. What would have taken months for Schwan's employees to learn took Barry a day and a half.

12.1.2 Spy Techniques and Prevention

Marc Barry is not the only one out there who can be a convincing actor when necessary. Ira Winkler, a former National Security Agency analyst turned corporate espionage expert, employs similar tactics. Unlike Barry, however, Winkler is not trying to steal the information for a competitor, but is trying to see how secure companies are so they know what areas they need to concentrate on for security purposes. In

one company, Winkler was able to gain entry to the building by telling a security guard that he had forgotten his work ID, but presented a business card that he claimed was his. In reality, he had stolen the card from a prize jar at a local restaurant. He proceeded through the building finding unlocked doors, forging signatures, and performing simple computer hacks. In the end, he had quickly and easily accessed design plans for nuclear reactors and even detected hackers in India trying to access the company's computer system.

The success of these individuals makes it obvious that corporate spying can be detrimental not only to a target company, but also conceivably to national security as well. Winkler reminds companies that "You can protect a computer perfectly, but if someone throws out a classified print out, you are out of luck." Spies can do just as much or more damage with social engineering as they can with computer hacking.

12.2 No Business Is Safe

In today's world, information theft is a growing concern. Perpetrators of this crime do not discriminate; they target large corporations, small businesses, and individuals equally. Tech-savvy and organized criminals alike have found ways to commandeer personal and banking information in order to make money at the expense of their targets. The methods of obtaining this information are as varied as the criminals themselves.

Although it is true that these criminals will target a person on an individual level, the biggest risk recently has been demonstrated by the security breaches within banks and larger corporations. On May 23, 2005, Bank of America and Wachovia were two of the major banks that came forward to tell more than 670,000 of their customers that their personal information had been compromised by employees within their organizations. Orazio Lembo approached employees offering them $10 per name if they would provide him with the personal information of account holders. He then used that information to pose as a collection agency, selling the information to law firms and collection agencies.

On May 31, 2005, less than one week after Bank of America and Wachovia made their announcement, police in Israel reported a

"massive industrial spying ring" that utilized Trojan-horse software to target major companies in Israel. The Trojan that was used infected the target machines, giving the programs designers, Michael Haephrati and Ruth Brier-Haephrati, information to their competitors' computers, FTP servers based in both Israel and the United States, and confidential information from competitors' machines. Despite the measures taken to prevent this type of theft from happening, the companies that were affected were not the first to come forward. The case was actually broken open when author Amnon Jacont found passages of a book he had been writing on the Internet, although he knew the passages had never left his computer.

Criminals taking advantage of big business were rampant in 2005. In February 2005, Alpharetta, Georgia-based ChoicePoint Inc. came forward to admit that the company had unknowingly sold Social Security numbers and other personal information to criminals. In June of that same year, Card Systems Solutions in Atlanta, Georgia, admitted that hackers had gained access to its system. In August, Sunbelt Software researchers came forward when they stumbled on CoolWebSearch, a spyware program that was found to upload information from personal computers to a central database. The information included chat sessions, eBay account information, usernames, and passwords. Between February and July 2005, more than 45 security breaches were reported to Privacy Rights Clearinghouse in San Diego.

Although banks and businesses are trying to stay on top of the risks presented by these and other criminals, they are finding that this is an almost impossible task. As the technology designed to protect information is evolving, so are the criminals. These criminals will keep trying to hack into the systems or find other ways in, and it is being found that the more complex the technology becomes, the more holes it is opening up for these individuals.

12.3 International Organization for Standardization Guidelines

One of the biggest challenges in setting up a new system for sensitive information is finding out where to start. The International Organization for Standardization (ISO) exists to verify standards, and the information they verify can be of great help to businesses

seeking to improve their information security standards. By following standards set in the ISO 17799 report, you will at least have a basic guideline on where to begin. Depending on the size of your company, exactly what is needed in your procedures will vary. It is often necessary to seek the help of a professional security consultant. As with any human venture, there exists among security professionals a small criminal element and a more broad number of ineffective *experts* and those who practice only to secure their own standard of living. You must be careful when choosing a private company to help with your security needs.

12.4 Choosing a Security Company

Look for a company or an individual that

- Has experience and specialty with your specific needs. If you are primarily an online merchant, then you will need someone with specific experience in databases, payment processing, and other aspects of selling online. A law office would probably not need someone who specializes in online credit card security.
- Has training from a solid institution. College education from an accredited university would be preferable, because there are many *buy a degree* programs online. Do not be fooled by claims of training and education from offshore schools and exclusively online companies. Any sort of military experience and training is also a plus, because this is also standardized. Check out the training institutions where the consultants you are considering had their training! A good way to do this is to Google *"college/training course name" Scam*. Keep the quotation marks around the name of the college/training course name so that you search most efficiently.
- Clears a basic online background check. How do you do this? CriminalCheck.com is a great place to start, because it is a free searchable database of sex offenders. You should also search for the individual or company the same way you did their educational institution, in quotes, with the word *scam* outside of quotes. If many variations are coming up, try searching for

the name in quotes, and the city/state in quotes so that it looks something like this: "*First name Last name*" "*Freeport, NY.*"

- Offers references and a list of previous clients. The importance of references is debatable because they can be faked. However, if the security consultant you are considering has or is able to give you a list of previous clients, check them! Inquire with anyone mentioned on the website or résumé that they claim to have worked with.
- Other things to consider: How familiar is this company or individual with the ISO 17799 and ISO 27001? Do they even know what these important codes are? What model of applied security do they believe most in? Can they talk extensively and intelligently? As with any professional contractor, the consultant you choose should accept payment in thirds or halves (a third at beginning of project, a third at a specified midpoint, and a third on completion—or half at the beginning of the project and the remaining half at the end).

12.5 Responding to a Security Breach

12.5.1 Act Quickly

If you find your company has an incident where security is compromised, you need to take action quickly. In general, regardless of which specific security model your organization is following, immediate steps need to be taken in order to identify, analyze, and gather evidence and contain, mitigate, eradicate, and refine your security policy.

12.5.2 ISO 20002 Standards

If you are following the ISO 20002 standards, then you need to

- Report information security events and weaknesses
- Report information security events as quickly as possible
- Report security weaknesses in systems and services
- Manage information security incidents and improvements
- Establish incident response tasks and procedures
- Learn from your information security incidents
- Collect evidence to support your actions

These are broad suggestions because of the wide scope of fraud, identity theft, and other types of security breaches. For a few places to begin, see the Bibliography at the end of this chapter.

Education and consistent following of security standards are the most important weapons against security breaches. If your organization's employees are informed, and security is regularly reinforced and reiterated, breaches are much less likely to occur.

12.5.3 Steps to Take

Despite all your efforts, the worst happens. Someone has infiltrated your organization and collected sensitive information. What do you do next? When a security breach is suspected, there are steps that need to be taken to stop internal and external attackers from stealing or damaging data.

12.5.3.1 Assemble an Incident-Response Team The first step, which should be done before a breach ever even occurs, is to assemble an incident-response team. The team not only should consist of the IT department, but also should include legal experts, top executives, public relations people, and representatives from all of the business lines affected. If the breach involves insiders, someone from human resources will be needed on the team. If it involves money, a financial officer should be on the team.

A Computer Security Incident Response Team (CSIRT)—including external consultants or forensics experts—should be selected before an event. Teams may vary according to the nature of the incident.

12.5.3.2 Assess the Initial Damage and the Risk for More Your response to a security breach will be commensurate with the risks to your business. The costs of a breach should include not only the technical costs associated with finding and fixing the breach, but also loss of productivity and loss of business. A plan needs to be in place that not only outlines a strategy for recovering systems, but also includes steps for recovering customers. Brand loss can be the most damaging element in a customer-facing breach.

12.5.3.3 Develop a Notification Plan After an assessment of damage is completed, it is time to develop a notification plan. Decide who to tell and in what order. If a potential crime has been committed, law enforcement should be called first. If consultants such as security experts or a computer forensics firm is needed, they should be brought in as early as possible.

Informing employees of what is going on may require training. They will need to know how their systems may be impacted, and what to do—or not do—to protect them. Employees will need to be told what they can and cannot say to customers or others outside the company.

If the breach comes from outside the company, informing personnel is easier than if the suspected breach is an inside job. Who is told and how they are told can make a difference in whether the problem can quickly be found and fixed.

Notification also needs to be made public. In most states, laws are in place that allow up to 30 days for disclosure to customers and others who may be affected by the breach. In most cases, there will be time to work on the problem before a public statement is made.

12.5.3.4 Touch Nothing until a Forensics Team Is Called Remediation should not take place until the problem and its potential impact are fully understood. Nothing should be touched until a forensics team has been called in, or the risk of damaging the evidence may occur or make the problem worse.

If the breach is actively hurting your business, you will want to unplug the servers or storage systems that are being infected or penetrated in order to limit the damage. In the case of an Internet-borne breach, turning off Port 80 might help.

Smaller companies would do well to wait for expert teams to come in before taking any action. Some larger companies have trained forensic staff in house.

Some problems do not immediately present themselves as security incidents, and IT staff may have already treated them with everyday troubleshooting measures.

12.5.3.5 Document Everything This is a very crucial step that should not be ignored—even if it is time consuming. Lack of documentation cannot only make it difficult to rebuild your systems after an

incident—it can also hurt your chances to make a case against an attacker in court. Throughout the assessment and remediation process, you should record everything, from how the incident was first detected to how the various members of the CSIRT responded.

In some cases—particularly in the case of attacks from outside the company—the documentation will be done automatically, through log files from firewalls, intrusion defense systems/intrusion prevention systems, and/or security information management tools. These tools should record the intrusion, the subsequent infections or downloads, and the configuration changes that were made to halt the attack.

An inside attack is not always detected initially through traditional security tools, but by someone noticing unusual or suspicious behavior. In these cases, it is important to document the reports and log the behavior in addition to using monitoring tools to track computer activity.

12.5.4 Stopping the Next Attack

To stop the next attack, a strategy needs to be developed to address the issues. If one attacker finds vulnerability, there is a good chance that there may be accomplices, or that another attacker might find the same vulnerability.

It is not unusual for attacks to come in bunches, so it is important to permanently seal off your leaks and decide how you will alter your response process if an incident occurs again.

12.6 Preventing Physical Theft

Here are tips for preventing physical theft at *brick and mortar* companies from David J. Shillingford's article "Lessons from an Equipment Thief":

- Thieves most fear getting caught when stealing, storing, or moving the equipment. The risk of getting caught when selling the equipment is considered low because owners tend to not record serial numbers, buyers of used equipment tend not to check titles, and even with leads, it is difficult for police to identify equipment and link serial numbers to owners.

- Sites tend to be either well secured or not—either because the worksite is impossible to secure or because of the attitude of the contractor. There are enough sites with poor security to keep thieves in business for years. It is not necessary to be 100 percent secure, but to be at least better than average, so thieves opt for the less-secure sites.
- There is no point in setting up security procedures that are either too complex or not regularly checked, as thieves will just watch and wait until security starts to decline.
- Employees of your firm and other local firms are both your best allies and biggest risks. They are the ones who will usually be responsible for the implementation of security and may even know something about a theft. They may even be the ones who let the thieves know about poor security. The key is to give them incentives to help rather than hinder.
- If you do not record your serial numbers, you can forget about getting your equipment back. Even if recovered, you still have to prove that it is yours. Better still is to find a way of making this information readily available to law enforcement and to use signs and decals to let the thief know this has been done.
- Getting help with setting up SSI procedures can be an overwhelming task, as can dealing with breaches in security. It is important to think critically and not neglect careful research when selecting a security consultant. Having a policy and trusted resources to refer to before a security incident happens is invaluable. Consistently apply company security policies, and educate yourself and company personnel to prevent security breaches.

12.7 Security Breach Notification Laws

Not every state has a security breach notification law, and in those states, companies are not required to let consumers know if they were affected by a breach. However, today most companies that have experienced security breaches involving sensitive personal information are notifying the affected individuals (www.privacy-rights.org). According to www.consumersunion.org, as of April 20, 2007, the 36 states that have security breach notification laws include Arizona,

Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, Wisconsin, and Wyoming.

12.7.1 Example of a Notification Law

Below is an example of a Notification Law.

> California—Civil Code Sec. 1798.80–1798.82, effective July 1, 2003, requires notice to consumers of a breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by a business or a government agency. If a business has its own notification procedures consistent with requirements and provides notice according to its policies or if a business abides by state or federal law provides greater protection and disclosure, then deemed in compliance.

If your state does not have a security breach notification law, you may wish to contact your legislators and ask them to enact such a law.

The Privacy Rights Clearinghouse (PRC) keeps a running list of the many data breaches that have been reported. PRC limits the list to only those breaches that involve personal data that could be used to commit identity theft such as Social Security numbers and financial account numbers. The link to PRC's chronology of security breaches is www.privacyrights.org–ChronDataBreaches.htm.

PRC says the list is not comprehensive. There are certainly more security breaches than those listed. PRC adds breaches to the list when it learns of them in news stories and from individuals who have received breach notice letters.

For a detailed explanation of the California breach notification law, see Appendix D.

12.7.2 Notification Process

Notification is likely to apply only if the breach involves sensitive personal information that could be used by an identity thief to commit

fraud, such as stealing Social Security numbers and financial account numbers.

12.7.2.1 California Office of Privacy Protection Recommendations The California Office of Privacy Protection has developed a series of recommended practices for California companies, government agencies, nonprofit, or educational institutions. The steps outlined for California are likely applicable in other states as well. If you are located in a state with a security breach notice law, contact your Attorney General's office for guidance on what to do.

California's recommendations for notification suggest that the type of information that requires notification includes unencrypted computerized data including certain personal information; personal information that triggers the notice requirement is name (first name or initial and last name); plus any of the following:

- Social Security number
- Driver's license or California Identification Card number
- Financial account number, credit or debit card number (along with any PIN or other access code where required for access to account)

Notice must be given to any data subjects who are California residents. Notification should be timely and as quickly as possible without delay. However, extra time may be allowed for law enforcement to conduct a criminal investigation and/or for taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system. Notice may be provided in writing, electronically, or by substitute notice. Substitute notice may be used if the cost of providing individual notice is more than $250,000, more than 500,000 people would have to be notified, or the organization does not have sufficient contact information for those affected.

Substitute notice includes e-mail when the e-mail address is available, and conspicuous posting on a website, and notification of major statewide media.

Alternatively, the business or agency may use its own notification procedures as part of an information security policy for personal information, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Dear _____:

We are contacting you about a potential problem involving identity theft. (Describe the information compromise and how you are responding to it.)

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax 800-685-1111
Experian 888-397-3742
TransUnionCorp 800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call (insert contact information for law enforcement) and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.consumer.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's identity theft data clearinghouse, where it will be accessible to law enforcers for their investigations.

(Insert closing)
Your name

Figure 12.1 Model letter for the compromise of social security numbers.

12.7.2.2 Model Letter Figure 12.1 shows a model for notifying people whose names and Social Security numbers have been stolen. In cases of stolen Social Security numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft should also review their credit reports periodically to keep track of whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

12.7.3 Federal Trade Commission (FTC)

This publication provides general guidance for an organization that has experienced an information compromise. If you would like more individualized guidance, you may contact the FTC at idt-brt@ftc.gov. Please provide information regarding what has occurred, including the type of information taken, the number of people potentially

affected, your contact information, and contact information for the law enforcement agent with whom you are working. The FTC can prepare its Consumer Response Center for calls from the people affected, help law enforcement with information from its national victim complaint database, and provide you with additional guidance as necessary. Because the FTC has a law enforcement role with respect to information privacy, if you prefer to seek guidance anonymously, you may do so.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. To file a complaint or to get free information on consumer issues, visit http://www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the United States and abroad.

12.8 Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to http://www.sba.gov/ombudsman.

13
ANSI Standards

13.1 The ANSI INCITS 359-2004

The ANSI INCITS 359-2004 is a specific Role-Based Access Control (RBAC) standard of information security created by the International Committee for Information Technology Standards (INCITS) and formally approved by the American National Standards Institute (ANSI) in April 2004. The full name of this standard is *ANSI INCITS 359-2004, American National Standard for Information Technology & Role Based Access Control*.

13.1.1 RBAC

RBAC was formalized in 1992 by David Ferraiolo and Rick Kuhn and has quickly become the predominant model for advanced access control, and it has been adopted into many security systems. RBAC, as standardized in the ANSI INCITS 359-2004 reduces the complexity and cost of security administration in large networks. RBAC was originally intended for mainstream commerce systems, but is finding application in areas as diverse as healthcare and military. Most information technology vendors now incorporate RBAC into their product lines.

RBAC is the means by which the ability to access information is explicitly enabled or restricted in some way, based on the roles that individual users have in an organization. These controls may be implemented in the computer system or in external devices.

In RBAC, access rights are grouped by role name (such as the roles of teacher and principal), and the use of information is restricted to individuals authorized to assume the associated role. For example, within a school system, the teacher would have access only to

information about students in his or her classroom, and the role of principal would have access to information on all students.

This can be an effective way to streamline security measures and protect SSI. User membership in roles can be updated, and role privileges changed without updating the privileges for every user on an individual basis.

13.2 ANSI INCITS 359-2004 Organization

The ANSI INCITS 359-2004 is organized into two parts: the reference model and the functional specifications.

13.2.1 Reference Model

The reference model defines basic RBAC elements, relations, and functions. This serves the purpose of providing a consistent language and precisely defining the scope of the elements that are included in the standard.

13.2.2 Functional Specifications

There are four components of functional specifications that define requirements over administrative operations for the creation and maintenance of RBAC element sets and relations. These components are as follows.

13.2.2.1 Core RBAC These are the essential elements of the RBAC and include requirements that user-role and permission-role can be many-to-many as well as one-to-one. An example is that user *Betty* can have more than one *role* (i.e., doctor and researcher) and each role can have more than one permission (i.e., access to patient medical histories).

13.2.2.2 Hierarchical RBAC A hierarchy can be mathematically described as a partial order defining a seniority relationship between roles, whereby senior roles acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors. Thus,

the *principal* role would be higher than a *teacher* role and have permission to all privileges granted under the role of *teacher*.

13.2.2.3 Static Separation of Duty (SSD) Relations These enforce constraints on the assignment of users to roles and place restrictions on sets of roles so that if a user is assigned to one role, that user cannot be a member of a second role. For example, if one role requests expenditures (i.e., event planning) and another approves them (i.e., accounting), the organization may prohibit the same user from being assigned to both roles. Furthermore, this concept builds on the hierarchical component of RBAC, according to David F. Ferraiolo. Because of the potential for inconsistencies with respect to SSD relations and inheritance relations of a role hierarchy, we define SSD requirements in both the presence and the absence of role hierarchies:

- SSD in the Absence of a Hierarchy—SSD relations place constraints on the assignments of users to roles. Membership in one role prevents the user from being a member of other roles, depending on the SSD rules enforced.
- SSD in the Presence of a Hierarchy—This type of SSD relation works in the same way as basic SSD except that both inherited roles and directly assigned roles are considered when enforcing the constraints.

13.2.2.4 Dynamic Separation of Duty (DSD) Relations Like the SSD relations, these limit the permissions that are available to a user—however, DSD requirements limit the availability of the permissions by placing constraints on the roles that can be activated within or across a user's sessions. This operates on the principle of least privilege, meaning that each user has different levels of permission at different times and depending on the specific task being performed. This is often referred to as *timely revocation of trust*. In other words, DSD allows a user to be authorized for roles that do not cause a conflict of interest when acted on independently, but which could produce concerns when acted upon simultaneously. For example, during a convention, a user with the role of *promoter* could temporarily be given the permission to read past sales data, but would not be able to input new data.

13.3 ANSI INCITS 359-2004 as the RBAC Standard

RBAC continues to evolve, and ranges from being very simple to extremely sophisticated. It is used in many types of organizations to simplify administration of security policies, such as those based upon the framework of the ISO 27001.

The ANSI INCITS 359 can be regarded as the fundamental RBAC standard. It defines a consensus model of RBAC that can be used in a full range of applications. According to product description, these standards are " … intended for software engineers and product development managers who design products incorporating access control features; and managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functions."

Note that the official standardization of RBAC, the ANSI INCITS 359-2004, is a copyrighted document, and it is highly recommended that you legally purchase a full copy from a reputable source.

Bibliography

An introduction to role-based access control. Retrieved June 22, 2007, from http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html.

Ferraiolo, D.F. (2001, August). Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security*, Vol. 4, No. 3. Retrieved June 22, 2007, from http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf.

Ni, W. (n.d.). *NIST Standard for Role-Based Access Control*. Retrieved June 22, 2007, from http://engr.smu.edu/~rewini/5-7339/wenyi.ppt.

Role based access control. Retrieved June 22, 2007, from http://csrc.nist.gov/rbac/.

14

Corporate National Institute of Standards and Technology (NIST)

14.1 The Importance of Using the National Institute of Standards and Technology (NIST)

Businesses must ensure that they practice due care and due diligence with their security programs. They must implement non-technical security controls as well as policies and procedures to support the technical solutions used in the business. The NIST special publications and methodologies are helpful to ensure that commercial companies and state and federal systems are secure. Using NIST comprehensive methodologies for risk assessments helps ensure due care and due diligence above other methodologies such as the ISO 17799 and self-directed Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology.

Businesses cannot afford breaches of security, as they could lose data, market share, and current and potential clients, and they might never recover. They could even end up in court trying to demonstrate that they implemented the steps necessary to keep information secure. To avoid all of these potential problems, businesses must implement strong security management programs that include technical solutions as well as security processes and procedures. Without proof of due care and due diligence in a security program, a business loses the ability to substantiate its case.

14.2 Due Care and Due Diligence

The terms *due care* and *due diligence* are often used interchangeably; however, they are two distinct activities.

14.2.1 Due Care

In regard to security, *due care* represents the measures taken to demonstrate that an organization has assumed responsibility for the actions used to protect that organization and its resources.

14.2.2 Due Diligence

Due diligence reflects continual activities used to ensure that protection mechanisms that have been put into place are maintained and operational. For example, placing a firewall in front of your network can provide evidence of due care; however, it does not demonstrate due diligence. Due diligence would entail the refinement of the firewall rules and the occasional structured testing of the firewall rules to ensure that they cannot be circumvented.

14.3 Processes and Methodologies

Businesses that possess and process information must protect that information to ensure that the data maintained by the organization are not altered, not released to unauthorized persons, and kept confidential and available to authorized users when it is needed. Information that must be protected includes addresses, phone numbers, credit card numbers, bank account information, Social Security numbers, and any other information the business would not want released to unauthorized persons. Any personally identifiable information that could be used for identity theft or other malicious purposes must always be adequately protected.

Businesses have installed devices or software to protect networks, systems, and users as a defensive measure in order to help eliminate unnecessary network traffic on corporate networks and to protect systems from viruses/worms, spam, and spyware. Virtual private networks and virtual local area networks have been deployed to

protect information in transit and to segment users from each other. Separate network zones may have been created to protect development, production, and Internet facing systems from each other and from outside intruders. Unfortunately, most businesses believe these measures fully protect their information systems from tampering and that they protect their data. However, hardware and software alone does not provide all of the necessary security measures that must be employed in a business environment to protect information and systems.

Despite implementing extensive technical protective measures, only a fraction of these types of solutions represent the activities required to adequately safeguard information and systems. A business must employ additional nontechnical security controls and processes to help ensure that security vulnerabilities are mitigated to an acceptable level as well as to prove the business has exercised due care and due diligence in regard to security. In order to better secure an organization's network and data, the supporting managerial and operational security controls must be in place. The security documents created by the NIST will help.

14.4 Advantages of Using NIST

14.4.1 Useful for Proving Due Care and Due Diligence

NIST special publications and methodologies are extremely useful in proving due care and due diligence. The NIST documents were developed for federal systems, but they represent robust security controls businesses should adopt to protect networks and systems.

14.4.2 A More Thorough Approach

The NIST security controls provide a more thorough approach and detailed methodology than the ISO 17799, which is written toward commercial industry and the self-directed OCTAVE methodology. NIST special publications can be used to establish a security program, create contingency plans, develop system security plans, and provide detailed information on implementing security controls. NIST can be used to conduct security testing of applications and networks as well.

14.5 Conducting Risk Assessments

One of the most important security tasks that NIST can assist with is conducting risk assessments. The main advantage of using the NIST security methodology for risk assessments is that the process not only identifies threats to business operations and vulnerabilities within an organization, but it also provides specific quantifiable measurements of the impact of a vulnerability being exploited, therefore making a cost–benefit analysis of any recommended control easier. Additionally, the likelihood of an exploit being exercised and the residual risk to the network, system, or organization are quantified using NIST as well.

14.5.1 Perform Periodically

Periodic risk assessments of the business practices and technical measures that surround the security of a system or group of systems are a cornerstone of security management and must be conducted. Using the NIST process for conducting these risk assessments is essential to help ensure that due care and due diligence is practiced. If your business must comply with federal mandates such as the Sarbanes–Oxley Act, the Gramm–Leach–Bliley Act, the Health Insurance Portability and Accountability Act, and other regulations or you are looking at making a structured best effort in your security program, NIST special publications and methodologies will help ensure that you protect your business from security problems in the future. Using NIST will demonstrate the serious approach you take to security and that safeguarding and protecting data is of paramount importance to your business.

14.5.2 Maintain Records

Maintaining records of NIST-based risk assessments and remedial actions as well as the other NIST processes increases your ability to prove due care and due diligence with your security practices.

14.5.3 Use an Outside Security Company

When conducting a risk assessment, an outside organization should be used. Having a third party evaluate your security controls ensures that

the assessment is entirely objective and the results are unbiased and do not lean favorably toward one business unit over another because of internal pressures. A well-reputed security company with certified security experts who understand the NIST process and overall security practices must be used in order to substantiate that due care and due diligence are practiced.

14.5.4 Use Continuously

In order to be effective, any risk assessment process must also be a continuous effort. Security risk management using NIST guidance should be practiced and ingrained into the System Development Life Cycle for Information Technology systems as well as the organization's culture. Security risk management should not be performed because of requirements or regulations, but because it is a sound security practice directly supporting the business objectives and mission of the organization.

15
Cybersecurity

15.1 Information Storage and Transmission

15.1.1 Radicati Group

E-mails have revolutionized the way the business world communicates. The Radicati Group estimates from information in the first quarter of 2006 that the number of e-mails sent each day is 171 billion. That averages to 28.5 e-mails sent each day by every man, woman, and child on the planet! The volume breaks down further to 2 million e-mails sent each second, with 70%–72% being spam and viruses. Genuine e-mails come from only 1 billion people of the earth's 6 billion population.

15.1.2 School of Information Management and Systems (SIMS) Study

The information being stored electronically is so large that it is difficult to comprehend. A study published in 2003 by the SIMS at the University of California at Berkeley reports that

- There are five billion instant messages sent every day.
- During the year 2002, all information created worldwide amounted to 5 exabytes of new information, and 92% of the new information was stored on magnetic media, mostly on hard drives. That figure would be much larger today. The SIMS report estimated that amount of new information produced in 2002 was double the amount produced in 1999.
- Hard disks store most new information. Ninety-two percent of new information is stored on magnetic media, primarily hard disks. Film represents 7% of the total, paper 0.01%, and optical media 0.002%.

- The United States produces about 40% of the world's new stored information, including 33% of the world's new printed information, 30% of the world's new film titles, 40% of the world's information stored on optical media, and about 50% of the information stored on magnetic media.
- The World Wide Web contains about 170 terabytes of information on its surface; in volume, this is 17 times the size of the Library of Congress print collections.
- Published studies on media use say that the average American adult uses the telephone 16.17 hours a month, listens to radio 90 hours a month, and watches TV 131 hours a month. About 53% of the United States population uses the Internet, averaging 25 hours and 25 minutes a month at home, and 74 hours and 26 minutes a month at work—about 13% of the time. We offer these eye-opening statistics to prove a point—we are in the middle of an information explosion. It is happening worldwide. It is happening in your business or agency, and it is happening at your home.

15.1.3 Information Measurement Explained

A byte is the smallest standard measurement of storage. A kilobyte is about 1000 bytes, and 2 kilobytes can store about a typewritten page. The measurements continue upward in units that grow by 1000 through the megabyte, gigabyte, terabyte, petabyte, and exabyte. An exabyte is equal to 1,000,000,000,000,000,000 bytes.

The entire 19-million-book print collection of the Library of Congress would fit on only 10 terabytes of space. The SIMS study reports that the 5 exabytes produced in 2002 alone could hold the equivalent of text for all the words ever spoken by human beings. It would also be the equivalent of half a million new libraries the size of the print collection of the Library of Congress.

15.2 Cybersecurity Challenges

15.2.1 Securing Large Amounts of Information in Various Locations

It is not uncommon for a single computer workstation to have a terabyte of storage capacity. A large business/agency could easily have the

capacity to store information equal to the print collections of the Library of Congress. That is the first challenge of creating a secure environment for sensitive information—there are so many locations where huge amounts of it can exist. The information can be stored on live sources, such as a hard drive, or it can be archived on DVDs or tape drives.

15.2.2 Securing All Workstations

The second challenge is keeping information secure on each of your workstations. Portable storage devices such as external drives that can fit in a briefcase can store terabytes of data—flash drives that can fit on a keychain can hold gigabytes. The technology makes it easy for vast amounts of information to be harvested from a single unprotected workstation.

15.2.3 Securing Electronic Forms of Communication

The third challenge is to secure electronic forms of communication. Your sensitive information can leave your workplace through such avenues as e-mail, FTP connections, and through outside hacking. Each information source at your workplace that has Internet access should be considered vulnerable. No matter what kind of firewall you use, there are thousands of hackers with genius IQs who have the capability of getting through it. Even computers without direct access to the Internet can be vulnerable if they are connected by a network to computers that do have Internet access.

15.3 Protecting Your Most Sensitive Information

Just about every business or agency has information so sensitive that its loss, compromise, or theft would be catastrophic. For instance, your business may depend on a database of customer information that is so important that its loss could put your company out of business. The database, of course, serves no function unless it is used, so your customer service and marketing employees will all need access to it. Those employees, in order to be productive, must have access to technological tools such as the Internet and e-mail.

If your database is so sensitive that its theft would cause irreparable harm, then you have no choice. To guarantee maximum security, the database must exist on a system that is completely separate from any network that contains computers with Internet access.

15.3.1 Maintaining Two Computer Systems

Some agencies and companies protect their sensitive information by having two separate internal computer systems. The secure system might be mainframe-based, which means that the employees work only on dummy terminals.

15.3.1.1 Benefits This greatly reduces the chance that a dishonest or careless employee might sell or let gigabytes of information fall into the wrong hands. Dummy terminals generally do not have such things as USB or FireWire ports, so portable storage devices would be useless.

The critical information would be left on the mainframe—much more secure from insider copying and outside attack. It also must be backed up, both on-site and off-site. A company or agency would be foolish to keep its critical backed-up information in only one building. If that building is burned down, blown away, blown up, or otherwise destroyed, then the critical information would be lost. So the archives must be secure, perhaps involving transfer by hand of tape drive tapes from one location to the next. Making the transfer would be a vulnerable time. No system is perfectly safe.

The mainframe security system exemplifies Mark Twain's famous advice: "Put all your eggs in one basket—and watch that basket!"

15.3.1.2 Drawbacks The drawback to this is the cost of maintaining two systems instead of one. Even large corporations may balk at it, gambling that an increase in insecurity is an acceptable trade-off for the cost of two computer networks. As stated before, computer safeguards such as firewalls can greatly lessen the chances of information being lost or stolen, but they cannot guarantee safety. Information on computers with access to the Internet, or that have communication ports such as USB and FireWire, is much less secure than information on a mainframe-based system.

Unfortunately, many government institutions operating through congressionally approved tight budgets often sacrifice security for cost savings and convenience. Even critically sensitive information such as data from a nuclear research facility has been put at risk because of wayward laptops or lax security (see the Wen Ho Lee case in Chapter 5).

15.3.2 Minimum Precautions

If you must keep your information on a network that has Internet access, then consider taking these minimum precautions:

- Establish an up-to-date firewall and be cautious with it. It is much better to err on enacting tight restrictions than it is to err on not using enough restrictions.
- Use the best virus protection software available. Most importantly, keep it updated. New viruses are being invented every day by hackers who are probably smarter than the programmers who guard your network, or who write your antivirus software, for that matter.
- Disable all nonessential communication ports. Think of them as spigots that can easily be opened to let information poor out.
- Never let your critically sensitive information exist on a laptop. If your chief executive demands that he or she have a laptop with the information, and you cannot change his or her mind, then use state-of-the-art encryption techniques. If you know that a supervisor is violating policy or law by having improper access, then be prepared to take your case to a higher authority. Every security professional should know by heart the rules that govern information access. Before an improper request is made, you should lay the groundwork by knowing whom to contact and how to file a report. If the information pertains to national security, then it is your duty to report policy violations, no matter what the implications to your job might be.

15.4 E-Mail

We have already described the massive amounts of e-mails that go out each second. E-mail is a great tool that has enhanced productivity worldwide, but it can be dangerous to information security.

15.4.1 Potential Dangers of E-Mail

Any business or agency that has used an e-mail system for long will have experienced problems. An employee might accidentally send a scathing critique of her boss to him by hitting the Reply All button instead of the Reply button.

Every public e-mail address will eventually find its way into a spammer's database. Unless users are careful about the way their addresses are published, a new e-mail address will start being targeted by hundreds of spam e-mails a day in only a few months. Every day you can expect to be targeted by viruses, scams, and offers for erectile dysfunction medication. Even if you are careful, then anyone you have ever sent an e-mail to who is not careful can be infested by a virus that will harvest your e-mail address and send it to spammers.

The subject of illegitimate e-mail use, as vast as it is, should be considered by lawmakers for reform. Security in the global e-mail system is practically nonexistent. Anyone anywhere can send an anonymous e-mail, or much worse—an e-mail with a fraudulent return address.

15.4.2 Different Types of E-Mail

15.4.2.1 Company E-Mails Your company or agency likely has many e-mail addresses. Some addresses might lead to departments, while others go to individuals. If they are official e-mail addresses, your company has at least some control over them.

The e-mails come into your Simple Mail Transfer Protocol (SMTP) server, where they are likely stored in some way and sent to the intended destination. When an employee sends an e-mail, it goes first to your SMTP server, where it can be stored, and then it is routed on to its destination either inside or outside the building.

15.4.2.2 Monitored Company E-Mail A recent study reported that about a third of all United States companies read e-mail from employees. They can do this because the e-mail is sent using company equipment and software, which are to be used for company business only.

Letting your employees know that their e-mail is being monitored can serve as an incentive to use company e-mail only for company use.

Knowing that their e-mail is being watched will make employees less likely to violate security policy.

15.4.2.3 Outside E-Mail Accounts Many employees have a way of getting around the security of the official e-mail system. Employees may choose to use a web-based browser such as Gmail or Yahoo mail. The message does not go through the company SMTP system, so it is less likely to be intercepted and reviewed by management.

Gmail allows for storage of gigabytes of e-mails, enough space for years of sent and received e-mails for average users. The e-mails are searchable using the same search engine that Google uses, so they are conveniently accessible from anywhere. That convenience comes at a price in terms of security. Your sensitive e-mails become accessible to anyone who can hack into your username and password. Also, your company's sensitive e-mails wind up being stored on the servers on an outside business—not a good way to store important trade secrets.

15.4.3 The Dangers of Bypassing Official E-Mail Systems

15.4.3.1 White House Example In March 2007, it was discovered that White House officials had used non-government e-mail servers, mainly AOL and Gwb43.com (a domain owned by the Republican National Committee), to send potentially sensitive information (specifically discussing the firing of U.S. Attorneys).

The fact that government personnel bypassed official (and presumably secure) e-mail systems to send potentially sensitive information in the Alberto Gonzales controversy is a prime example of how the White House and United States government share many of the same communications security issues as corporations. The White House provides many lessons in e-mail management practices and using non-business e-mail accounts to conduct business.

15.4.3.2 Unsecure Servers Regardless of whether it was intentional to bypass government archiving and official record—e-mail servers such as AOL, Yahoo, MSN, and even domain-name level servers, are notoriously unsecured. Do a simple web search for e-mail hack and hundreds of relevant search results and tutorials appear on how to break into various types of e-mail accounts.

15.4.3.3 Specific Problems When employees and officials bypass official e-mail systems, it creates several significant problems:

- Others may be able to access business e-mail that contains sensitive and confidential information. If personnel download communications to their personal computers, those who are unauthorized (such as the employee's family and friends who use their personal computer) may be able to access such information.
- The personal e-mail system may not be secure, leading to such things as having customer and personnel e-mails being harvested for spam or disk operating system or malware attacks. This is especially the case if the employee is accessing less-secure web-based e-mail or using a non-work computer. Keystroke logging software, contained in many computer viruses and spyware, can compromise security by stealing passwords, and it can record every e-mail sent by personnel on the infected computer. Such software has been put to legitimate use in controlled settings by employers to track personal use of corporate computers, but it can also be installed and used by hackers on less secure and personal computers.
- E-mails originating outside of secure messaging servers are notoriously easy to fabricate and it is difficult to prove who the original sender was. In fact, it is possible that e-mails found to have been sent through external mail servers may not have actually been composed or sent by the authors the e-mails purport to have represented.
- Communicating from personal e-mail accounts does not only look unprofessional, it also puts such communications out of the control of the organization, leaving the corporation or government without the ability to monitor or log such communications. This is what clearly happened in the Gonzales controversy.
- Personnel may mistakenly send personal, and possibly inflammatory, communications. This obviously has the potential to cause public image issues. When an organization has no control over such e-mails, unofficial communications may go undetected for much longer than if they were being monitored.

Problems that could be immediately resolved could blow up and create more complex, expensive, and publicly unflattering issues.

- Allowing such communications to be sent outside the corporate-controlled communications system could be viewed as not following a standard of due care to protect customer information, making the government or organization vulnerable to noncompliance with applicable laws and regulations. In the Gonzales case, it has been debated whether government staffers violated the Hatch and Presidential Records acts (laws intended to ensure that all official business is recorded). In the corporate spheres, bypassing controlled communications systems potentially subjects companies to civil actions from upset customers if bad things happen to their information as a result.

15.4.3.4 Emerging Technologies Further complicating issues surrounding the bypassing of official organization e-mail servers are new and emerging communications technologies:

- Voice over IP can be integrated into e-mail systems, as conversations can be recorded and attached as audio files.
- Instant messaging is often used to allow real time interactive business communications. If an organization attempts to save money and use a free service such as Yahoo, ICQ, MSN, or AIM, security issues can become even more complicated.
- BlackBerry and other mobile Internet devices (such as web-browser enhanced cellular phones) are used by a large number of business personnel to send and receive e-mails no matter where they are and at any time of day. Besides the inherent security issues of these devices, it would be a possible issue if the employee were accessing sensitive information on a BlackBerry from a crowded public place, such as a subway where unauthorized people could potentially read over the shoulder and thus access confidential information.
- Storage Devices—According to Rebecca Herold of Realtime-ITcomplaince.com, "Because of the highly distributed locations where data is now stored, it is likely many of the storage

locations are unknown, or are under the control of end-users who may be doing things with the data that can have huge impact in court and on the organization."

The evolving systems and technologies are certainly timesaving and efficient business tools. However, business leaders need to consider the archiving, retention, and discovery requirements that are involved with these technologies to ensure they are not unknowingly putting the business at information security, privacy, and/or legal risk with the ways in which the technologies are implemented.

15.5 Cyber Checklists

The following is a checklist for ensuring cybersecurity.

15.5.1 International Travel

- Does the local power supply match your system's requirements? Are electrical power transformers, filters, surge protectors, or uninterruptible power supply units available to protect your equipment?
- Does the government impose restrictions on the import of computer hardware and software into the country?

15.5.2 Environment

- Will the computer be used in a low humidity area where damage from static electricity may be sustained? Are carpets treated? Are humidifiers available?
- Will the computer be used in a hot, dusty climate? Are office temperature controls sufficient? Are dust covers available?

15.5.3 Physical Security

- Is the work area kept clear of soft drinks, coffee, and other liquids that when accidentally spilled, may damage the equipment?

- Are diskettes physically labeled and handled as directed by the manufacturer? Are sensitive diskettes sufficiently write-protected to avoid accidental or malicious damage or destruction?
- Are backup copies stored off-site?
- Is the computer sufficiently protected from acts of sabotage, tampering, and theft?
- Are modems (particularly those with an automatic answer feature) disconnected or powered off when not in use?
- Are film printer ribbons, sensitive printouts, and diskettes burned, shredded, or degaussed as appropriate to prevent inadvertent information disclosure?

15.5.4 System Security

- Are spare user-serviceable parts available in the event of failure?
- Are backup copies of software and data produced periodically?
- Has a backup system (contingency) been identified to continue critical operations in the event of a failure/disaster? Has it been tested?
- Are system hardware and/or software controls present to authenticate individual system users? Are passwords changed frequently and are they easily guessed?
- Is a security erase or file scrub program present on the system that will overwrite sensitive data on the hard disk when a file is deleted? Is it used?
- Are sufficient controls in place to prevent violation of manufacturer's copyright and license agreements?

15.5.5 Virus Protection

- Are software and data diskettes received from trustworthy sources?
- Is software received from outside sources scanned for computer viruses with current virus detection software? (United States Department of State Overseas Security Advisory Council)

15.6 Data Storage Tips

It is important to protect the data on portable devices as well as the device itself. Any device that is connected to the Internet, especially a wireless connection, is susceptible to network attacks. But there are things users can do to protect their data.

15.6.1 Use Passwords Correctly

Do not use options that let your computer remember passwords and do not use passwords that are easily guessed by thieves. Use different passwords for different programs.

15.6.2 Store Data Separately

Forms of storage include floppy disks, zip disks, CDs, DVDs, and removable flash drives (USB drives or thumb drives). Saving data on removable media and keeping it in a secure location, such as a suitcase instead of a laptop bag, can protect data even if the laptop is stolen.

15.6.3 Encrypt Files

Encrypting files will ensure that unauthorized persons cannot view data even if they can physically access these. Full disk encryption prevents a thief from starting the laptop without a passphrase. When encryption is used, it is important to remember passwords and passphrases—if forgotten or lost, you may lose your data.

15.6.4 Virus Definitions

To protect laptops and personal digital assistants, make sure to keep your virus definitions up to date.

15.6.5 Firewalls

While always important for restricting traffic coming into and leaving your computer, firewalls are especially important if traveling and using different networks. Firewalls can help prevent outsiders from gaining unwanted access.

15.6.6 CDs and DVDs

Make sure to back up any data you have on your computer onto a CD-ROM, DVD-ROM, or network. This not only ensures that you will still have access to the information if your device is stolen, but it could also help you identify exactly which information a thief may be able to access. You may be able to take measures to reduce the amount of damage that exposure could cause.

PART V
Government Security Needs

CHAPTER 16 The Intelligence Process
CHAPTER 17 The Law and Homeland Security
CHAPTER 18 The Department of Homeland Security (DHS) Structure

16
The Intelligence Process

16.1 Intelligence and Counterintelligence

Unprocessed information is chaos; intelligence is knowledge.

16.1.1 Intelligence Defined

Webster's Dictionary defines *intelligence* as "information, news … secret information, esp. about an enemy." It goes on to state that intelligence is "the capacity to acquire and apply knowledge." Although the former definition focuses on product and reflects the very imprecise view held by the majority of Americans, the latter definition focuses on process and comes closer to a more meaningful definition of intelligence, as understood and practiced by intelligence professionals today and for the past 50 years. The fact is that intelligence, when referring to the activity of governments or corporations, is indeed a complex concept. This section surveys the meaning and scope of intelligence in this context.

16.1.2 Intelligence versus Information

It is necessary to recognize the difference between intelligence and information. More than 400 years ago, Sir Francis Bacon observed that "knowledge is power." He had no idea that by the end of the 20th century, the world would be drowning in information—thanks to rapid advances in technology, particularly during the past 25 years. Indeed, today there are virtually no limits to the information available to anyone with a computer and an Internet hookup. Today, it is the ability to convert this avalanche of information into meaningful and relevant knowledge that defines power. With this in mind, a more accurate definition of intelligence as a process becomes possible—it

is a system for collecting, evaluating, and converting information into meaningful and relevant knowledge. In fact, most intelligence agencies across the modern world today are functionally organized to accomplish two core tasks: first, the collection of raw intelligence (information); and second, the evaluation and analysis of this raw intelligence, and the write-up in the form of relevant intelligence reports for dissemination to appropriate government policy makers (or corporate executives).

16.1.3 The Definition of Intelligence as a Process

This represents a process or a system for collecting, evaluating, analyzing, and converting multiple pieces of information into an intelligence report that is responsive to an articulated need. In the case of governments, that need is usually related to national security or other foreign policy concerns; in the case of corporations, that need may be related to the company's need to maximize its competitive position.

16.1.3.1 Generating a Requirement Government policy makers generate a requirement (such as what are North Korea's capabilities and intentions regarding nuclear weapons?). This requirement is sent to the intelligence community for action.

16.1.3.2 Collecting Information Next, the intelligence community tasks its resources to collect information on this specific requirement—this collection effort may extend to different agencies and include clandestine human source (HUMINT) reporting; electronic and signals data (ELINT and SIGINT); communications intercept (COMINT); publicly available information, commonly referred to as open source intelligence (OSINT); satellite imagery; and other sources. Worldwide information relevant to the requirement will be collected as raw intelligence and sent back for evaluation, analysis, and ultimate dissemination in an intelligence format (finished intelligence).

16.1.3.3 Evaluating and Analyzing The analysts evaluate the raw intelligence for reliability, credibility, and relevance. Information from one source is compared with information from other sources; reliability of each source is evaluated as is the credibility of each reporting source.

Overhead imagery of a site may be compared with atmospheric collection from the same area to determine what has or is occurring at a given location. ELINT, COMINT, and SIGINT may be available to add additional information to the equation. Multiple HUMINT source reporting may add yet another dimension, perhaps relating to plans and intentions.

16.1.3.4 Writing an Intelligence Report Once all source reporting has been collected, evaluated, and analyzed, it will be written up and submitted as finished intelligence responsive to the original requirement.

16.1.3.5 Dissemination This intelligence report is sent to the policy maker who asked the initial question. Thus, the intelligence cycle is completed.

16.1.4 Intelligence as a Discipline

While the above provides a working definition of intelligence as a process, it should be recognized that intelligence, when viewed as a discipline, takes on an even broader definition. Under this definition, intelligence encompasses such concepts as Covert Action (promoting a political goal), Disinformation (misleading information), Counterintelligence (protecting intelligence), Influence Agents (influencing foreign governments), and other resources and techniques that are part of the intelligence business. In short, when the government refers to *intelligence* as a resource, it has in mind not only the product and process, but also the entire array of intelligence tools and techniques specifically developed to support the foreign policy goals of the government and protect the national security of the country. Each of these aspects of intelligence warrants a separate discussion:

- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency (CIA)
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy

- Department of Homeland Security
- Department of State
- Department of the Treasury

16.2 Military Intelligence

The Army is one of the oldest intelligence organizations. However, the Army did not acquire a permanent peacetime intelligence organization until 1885 and did not formally recognize intelligence as a discipline until 1962. At that time, it created the Army Intelligence and Security Branch, the predecessor of today's Military Intelligence branch. According to military authors, "The Military Intelligence Corps, which incorporated all military intelligence personnel and units into a single large regiment, did not come into existence until 1987" (Finnegan, 1998).

Much of the military's intelligence training takes place at Fort Huachuca, Arizona, at the U.S. Army Intelligence Center and School. The U.S. Army Intelligence Officers and Noncommissioned Officers are primarily known for their high level of intelligence, often having IQs that place them in the top 10 percent of the population. Because of their exposure to foreign intelligence officers from non-friendly nations, military intelligence personnel go through an exhaustive selection process, frequent polygraph testing, and standards of conduct that are much higher than those of most regular military units, with the exception of special operation forces.

16.2.1 CIA Defines Intelligence

In 2007, the CIA defines intelligence as

> … the collecting and processing of … information about foreign countries and their agents which is needed by a government for its foreign policy and for national security, the conduct of non-attributable activities abroad to facilitate the implementation of foreign policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure. (Central Intelligence Agency, 2007)

Of all the U.S. military services, the Army is the only branch to separate traditional criminal investigators from national security crime investigators. Espionage, treason, and terrorism are crimes investigated only by the Army's counterintelligence agents. Crimes that are not related to national security are investigated by agents from the Criminal Investigative Command. Most military services have intelligence personnel who perform various intelligence-related job functions, including interrogation and technical security countermeasures or bug sweeping as in the Army. The Army, Navy, Marines, Air Force, and the U.S. Coast Guard each have their own intelligence personnel.

16.2.2 Intelligence Subspecialties

U.S. intelligence personnel are recruited into the intelligence profession and assigned to subspecialties as listed below upon selection:

- HUMINT (Human Intelligence)
- SIGINT (Signals Intelligence)
- COMINT (Communications Intelligence)
- ELINT (Electronic Intelligence)
- FISINT (Foreign Instrumentation Systems Intelligence)
- IMINT (Imagery Intelligence)
- MASINT (Measurement and Signatures Intelligence)
- RADINT (Radar Intelligence)
- IRINT (Infrared Intelligence)
- NUCINT (Nuclear Intelligence)
- ACOUSINT (Acoustic Intelligence)
- OSINT (Open Source Intelligence)
- CI (Counterintelligence)

Some specialties, such as interrogators and SIGINT, require proficiency in a foreign language, and therefore the intelligence training will include a short assignment at Defense Language Institute Foreign Language Center in Monterey, California.

All military intelligence personnel are trained in the process of intelligence. The process of intelligence has four phases: collection, analysis, processing, and dissemination.

16.2.3 Restrictions

Intelligence personnel are limited in what they can do and for whom they do it. Tasks performed by military intelligence personnel are restricted, undergo tremendous oversight, and are performed strictly for military use.

16.2.3.1 Posse Comitatus Act The Posse Comitatus Act is just one of several laws and directives in existence that prevent the military from doing anything outside of military jurisdiction, including military action or investigation against U.S. civilians. For example, even though military counterintelligence personnel are much like their CIA and Federal Bureau of Investigation (FBI) counterparts, they are restricted from collecting and investigating matters outside of military jurisdiction. If a U.S. civilian comes to the attention of military intelligence as a person of interest to a national security matter, the matter is turned over to the FBI.

16.2.3.2 Executive Order 12333 Executive Order 12333, signed by President Ronald Reagan on December 4, 1981, gives the intelligence community its authority to collect foreign and domestic intelligence and counterintelligence information relating to national security. This executive order updated a previous order originally signed by President Gerald Ford after U.S. intelligence agencies were caught collecting information on community, religious, and labor leaders; civil rights protestors; and anti–Vietnam War demonstrators (Arkin, 2005).

16.2.4 Other Agencies

Other agencies that produce and manage intelligence-related reports, products, and personnel for the military's use include the following:

- NSA (National Security Agency)
- DIA (Defense Intelligence Agency)
- NRO (National Reconnaissance Office)
- NGA (National Geospatial-Intelligence Agency)
- AIA (Air Intelligence Agency)
- INSCOM (Intelligence and Security Command) U.S. Army
- ONI (Office of Naval Intelligence)
- MCID (Marine Corps Intelligence Department)

Bibliography

Arkin, W. (2005, September). Another law under assault. *Washington Post*. Retrieved from http://blog.washington-post.com/earlywarning/2005/09/another_law_under_assault.html.

Central Intelligence Agency. (2007). A definition of intelligence. Retrieved August 10, 2007, from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v02i4a08p_0004.htm.

Finnegan, J.P. (1998). Military intelligence: Lineages compiled by Romana Danysh. Center of Military History, United States Army, Washington, DC. Retrieved from http://www.army.mil/cmh-pg/books/Lineage/mi/ch5.htm.

17
The Law and Homeland Security

17.1 Background

President George W. Bush authorized a domestic eavesdropping program after September 11, 2001. Since the surveillance program began, the United States has intercepted plots to destroy the Brooklyn Bridge, to smuggle missiles into the United States, and to detonate a fertilizer bomb in London (Risen and Lichtblau, 2005).

The president possesses broad powers in the protection of national security, including a power to formulate foreign policy. The president has intelligence information about national security issues that is generally unavailable to Congress. Congress passed legislation after September 11, 2001, that gave the president the specific power to eavesdrop on calls that suspected al-Qaeda operatives are making to the United States. The terrorist surveillance program is designed to protect against another terrorist attack.

17.2 Executive Summary

The Defense Department is deeply involved in domestic intelligence concerning threats to national security that unfold on U.S. soil. The department's NSA has been conducting, outside the framework of the Foreign Intelligence Surveillance Act (FISA), electronic surveillance of U.S. citizens within the United States. Other Pentagon agencies, notably the one known as Counterintelligence Field Activity (CIFA), have been conducting domestic intelligence on a large scale. Although the CIFA's formal mission is to prevent attacks on military installations in the United States, the scale of its activities suggests a broader concern with domestic security. Another Pentagon agency engaging

in domestic intelligence is the Information Dominance Center, which developed the Able Danger data-mining program.

The significance of these programs is in reducing gaps in our defenses against terrorism. The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy, but the Defense Department maintains that machine collection and processing of data cannot invade privacy. Due to the sheer volume, the data are first sifted by computers, which search for names, addresses, and phone numbers, or specific information that may have intelligence value. This initial sifting keeps most private data from being read by any intelligence officer. The data that make the cut are those that contain clues to possible threats to national security.

The FISA makes it difficult to conduct surveillance of U.S. citizens and lawful permanent residents unless they are suspected of being involved in terrorist or other hostile activities. Innocent people, such as unwitting neighbors of terrorists, may, without knowing it, have valuable counterterrorist information. Collecting such information is conceivable with data-mining projects such as Able Danger (Jasper, 2005).

The goal of national security intelligence is to prevent a terrorist attack, not just punish the attacker after it occurs, and the information that enables the detection of an impending attack may be scattered around the world in tiny bits. A much wider, finer-meshed net must be cast than when investigating a specific crime. Many of the relevant bits may be in the e-mails, phone conversations, or banking records of U.S. citizens, some innocent, some not so innocent. The government is entitled to those data, but just for the limited purpose of protecting national security.

17.3 History of Electronic Surveillance and FISA Court

17.3.1 Electronic Surveillance and National Security

With the invention of the microphone, the telephone, and the dictograph recorder, it became possible to eavesdrop with much greater secrecy and expediency. Inevitably, the use of electronic devices in law enforcement was challenged, and in *Katz v. United States* (1967), Justice White sought to preserve for a future case the possibility that in national security cases electronic surveillance

upon the authorization of the president or the attorney general could be permissible without prior judicial approval. The executive branch then asserted the power to wiretap and to conduct electronic surveillance in two types of national security situations, against domestic subversion and against foreign intelligence operations, first basing its authority on a theory of inherent presidential power and then in the Supreme Court withdrawing to the argument that such surveillance was a reasonable search and seizure and, therefore, valid under the Fourth Amendment.

The Supreme Court first confronted the tension between unmonitored executive branch surveillance and civil liberties in *United States v. U.S. District Court*, in which the United States charged defendants with conspiracy to destroy government property. Defendants sought suppression of electronic surveillance information held by the prosecution. The attorney general admitted that a warrantless wiretap had intercepted conversations involving the defendants. Before the Supreme Court, the government defended its actions on the basis of the Constitution and the Title III national security disclaimer.

The Court accepted that the president had the power to protect our government against those who would subvert or overthrow it by unlawful means and that this power justified electronic surveillance of would-be subversives.

17.3.2 FISA

The 1978 FISA defines the Justice Department's authority to conduct physical and electronic surveillance for foreign intelligence information. FISA provides two mechanisms to perform searches.

17.3.2.1 Warrants FISA authorizes the Justice Department to obtain warrants from the secret Foreign Intelligence Surveillance Court (FISC) up to 72 hours after the beginning of the eavesdropping.

17.3.2.2 Foreign Combatants FISA permits the president to authorize the Justice Department to conduct foreign intelligence surveillance for up to 1 year without a court order (50 United States Code 1802a(1)). The surveillance must be directed at communications used

exclusively by enemy combatants on foreign soil, not U.S. citizens. FISA applies to surveillance whose significant purpose must be for gathering foreign intelligence information, which is information necessary to protect against a potential grave attack, sabotage, or international terrorism.

Although FISA surveillances must have an intelligence purpose, courts allow FISA-obtained information to be used in criminal trials. However, FISA's minimization requirement mandates that procedures be implemented to minimize the collection, retention, and dissemination of information about United States persons. Minimization procedures are designed to prevent the broad power of foreign intelligence gathering from being used for routine criminal investigations. In a number of instances, however, there are overlaps between foreign intelligence gathering and criminal investigations. One common minimization procedure is what is known as an information-screening wall. These walls require an official not involved in the criminal investigation to review the raw materials gathered by FISA surveillance and only pass on information that might be relevant evidence. The purpose is to ensure that criminal investigators do not use FISA authority for criminal investigations.

17.3.3 Foreign Intelligence Information (FII)

FII is information that relates to United States ability to protect against possible hostile acts of a foreign power or an agent of a foreign power, sabotage, or terrorism by a foreign power or agent, and clandestine intelligence activities by a foreign power or agent. FII includes information with respect to a foreign power or foreign territory that relates to the national defense, national security, or conduct of foreign affairs of the United States. If the intended surveillance target is a U.S. person, the information must instead be necessary to protect against hostile acts, sabotage, or terrorism, or U.S. national defense, national security, or foreign affairs.

17.3.4 FISC

FISA established a special court, the FISC composed of seven federal district court judges appointed by the Chief Justice for staggered terms

and from different circuits. Individual judges of the FISC review the attorney general's applications for authorization of electronic surveillance aimed at obtaining foreign intelligence information.

17.3.4.1 Court Proceedings The FISC meets 2 days monthly. The proceedings are not adversarial; they are based entirely on the Department of Justice's presentations through its Office of Intelligence Policy and Review.

17.3.4.2 FISA Application Under FISA, the Justice Department reviews applications for counterintelligence warrants by agencies before submitting them to the FISC. The attorney general must personally approve each final FISA application.

The application must contain, among other things,

- A statement of reasons to believe that the target of the surveillance is a foreign power or agent of a foreign power, (subject to the relevant amendments made by the U.S. PATRIOT Act)
- A certification from a high-ranking executive branch official stating that the information sought is deemed to be foreign intelligence information, that the information sought cannot reasonably be obtained by normal investigative techniques
- Statements regarding all previous applications involving the target
- Detailed description of the nature of the information sought and of the type of communication or activities to be subject to the surveillance
- The length of time surveillance is required
- Whether physical entry into a premise is necessary, and proposed procedures to minimize the acquisition, use, and retention of information concerning non-consenting U.S. persons

17.4 Political Fallout of Electronic Surveillance

The American Civil Liberties Union (ACLU) and other civil libertarians are crying foul that the use of electronic surveillance undermines our civil liberties. These groups express their displeasure at

our nation's homeland security policies by arguing that the practices violate personal privacy. The continued use of electronic surveillance will be scrutinized and challenged and the argument will continue into the foreseeable future. Public opinion of the NSA program may be swayed to where more and more people oppose the program. The ACLU Washington legislative office clearly states that the NSA electronic surveillance program is illegal and that we as citizens must choose between our constitutional rights and our security (ACLU, 2006). The ACLU has already filed a lawsuit against the NSA and has stated that they believe the warrantless surveillance must end and checks and balances must be restored.

The Center for Democracy and Technology (CDT) has also weighed in on electronic surveillance and is on record as opposing the president's program through NSA. CDT has joined in the lawsuit with the ACLU against the NSA and has called on citizens to contact members of Congress and urge them to support a full inquiry in both the House and the Senate into domestic activities of the NSA before any legislation of any kind is considered having to do with homeland security.

17.5 Impact of Electronic Surveillance

The foremost goal of any intelligence program is to keep track of threats, events, and developments that are capable of threatening the nation's existence. There have been many instances over the years of direct terrorist attacks on a state in which at best the government was inadequately prepared and could not prevent the attack from occurring.

17.5.1 Foreign Intelligence

The purpose of foreign intelligence is to provide information to national security decision-makers so they can use the economic, political, or military power at their disposal more effectively. To accomplish this purpose, foreign intelligence agencies covertly acquire, analyze, and disseminate information regarding threats to national security. A covert information acquisition capability supplements overt information collection because much of international relations are conducted

in secret and the only way to apply power effectively in an area where so much is kept secret is by uncovering the capabilities and intentions of enemies and potential competitors. Democracies in this perilous world must have intelligence gathering capabilities. The United States could well perish at the hands of foreign enemies without the protection afforded by the eyes and ears of the intelligence community (Johnson, 1991).

17.5.2 Domestic Intelligence

Domestic intelligence serves the same purpose as foreign intelligence, to enable government power to be applied with greater precision, and it is structured in a similar way. Domestic intelligence can be defined as the collection, evaluation, and collation of information relating to threats to government, including threats to the orderly conduct of government business. As with foreign intelligence, the primary benefit of domestic intelligence is that it allows domestic security agencies to apply their powers of search, detention, and arrest with greater precision and less collateral damage. For example, informants can provide information leading to the arrest of people suspected of committing crimes, and wiretaps can provide law enforcement agencies with sufficient information to arrest suspects before they can carry out criminal or terrorist activities. Domestic intelligence can also provide correct information to law enforcement personnel so that misapplication of power, such as false arrests and breaking down doors to wrong houses, does not occur.

17.5.3 Security Threats

Terrorism has led to an increased need for domestic intelligence. In the future, the threat to homeland security will be even greater because of growth in technology, and as a result, the role of domestic intelligence in protecting homeland security will be even greater than it is today. The threat to security is growing because technological knowledge allows for greater power at less cost and requires the efforts of fewer and fewer people. Soon technological advances in areas including genetics and nanotechnology will require the reconceptualization of security. Biological warfare is bad enough, but biological

warfare incorporating genetic engineering is potentially apocalyptic. Information from the human genome could give biological weapons programs the means to target specific ethnic groups transforming biological weapons into potent tools of ethnic cleansing and terrorism (Anbarasan, 1999). The threat that this kind of weapon could pose to international peace and stability is incalculable. As technological capabilities become more advanced, the need to monitor smaller and smaller groups to prevent the development of new weapons by terrorists becomes increasingly important. In the end, prospects for comprehensive national domestic intelligence collection and exploitation have increased since the September 11, 2001, terrorist attacks, and the future need may be even greater.

17.5.4 NSA Monitoring

The need to have an electronic surveillance program in place is crucial if we are to infiltrate and prevent terrorist activity. The Authorization for Use of Military Force (AUMF), Public Law 107-40, 115 Statute 224, justified the monitoring of the NSA. The AUMF specifically authorized the president to use all necessary and appropriate force against those nations, organizations, or persons he or she determines planned, authorized, committed, or aided the terrorist attacks, or harbored such organizations or persons (Bazan and Elsea, 2006). There can be no doubt that individuals who fight against the United States in the Middle East as part of the Taliban, an organization known to have supported the al-Qaeda terrorist network responsible for 9/11, are individuals Congress sought to target in passing the AUMF. It is argued that the electronic surveillance of individuals falling into the limited category considered, for the duration of the particular conflict in which they are monitored, is so fundamental that it must be accepted as an incident to war and the use of electronic surveillance is an exercise of the necessary and appropriate force Congress has authorized the President to use (*Hamdi v. Rumsfeld* [03-6696] 542 U.S. 507, 2004).

Article II of the Constitution gives the president inherent authority as commander in chief to protect national security from foreign threats, and Congress cannot, by statute, inhibit that constitutional authority (Prize Cases, 67 U.S. [2 Black] 635, 668 1 863).

There is a national security exception to the Fourth Amendment that permits the government to conduct searches and surveillance for foreign intelligence surveillance. Wiretapping to protect the security of the nation has been authorized by successive presidents.

Bibliography

50 United States Code.

American Civil Liberties Union (ACLU). (2006, February 24). Majority recognize importance of checks and balances against abuses of power. *ACLU*. Retrieved February 26, 2005, from http://www.aclu.org/safefree/nsaspying//.

Anbarasan, E. (1999, March). Genetic weapons: A 21st century nightmare. *UNESCO Courier*.

Bazan, E. & Elsea, J. (2006, January 5). Presidential authority to conduct warrantless electronic searches. *Congressional Research Service*. Retrieved February 27, 2006, from http://www.fas.org/sgp/crs/intel/m010506.pdf.

Hamdi v. Rumsfeld (03-6696) 542 U.S. 507. (2004).

Jasper, W.F. (2005, October 31). Able danger & 9/11 foreknowledge. *The New American*. Retrieved February 9, 2006, from http://www.thenewamerican.com/artman/publish/article_2418.shtml.

Johnson, L. (1991). Controlling the CIA: A critique of current safeguards. In G.P. Hastedt (Ed.). *Controlling Intelligence*. London: Frank Cass.

Katz v. United States. (1967) 389 U.S. 347.

Risen, J. & Lichtblau, E. (2005, December 16). Bush lets U.S. spy on callers without courts. *New York Times*. Retrieved February 16, 2006, from http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5070&en=ffe9ca965d55805e&ex=1142830800&adxnnl=1&adxnnlx=1142700061-BCbJxv41N-MZifT9med1JOg/.

18

The Department of Homeland Security (DHS) Structure

The DHS offers the following explanation of its many parts and their functions.

18.1 Department Subcomponents and Agencies

Homeland Security leverages resources within federal, state, and local governments, coordinating the transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the federal, state, and local levels have homeland security responsibilities. The comprehensive national strategy seeks to develop a complementary system connecting all levels of government without duplicating effort. Homeland Security is a national mission.

This list contains the major components that currently make up the DHS.

18.2 Department Components

18.2.1 Directorate for National Protection and Programs

This works to advance the department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.

18.2.2 Directorate for Science and Technology

This is the primary research and development arm of the department. It provides federal, state, and local officials with the technology and capabilities to protect the homeland.

18.2.3 Directorate for Management

This is responsible for department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements.

18.2.4 Office of Policy

The Office of Policy provides the primary policy formulation and coordination component for the DHS. It provides a centralized, coordinated focus to the development of department-wide, long-range planning to protect the United States.

18.2.5 Office of Health Affairs

This office coordinates all medical activities of the DHS to ensure appropriate preparation for and response to incidents having medical significance.

18.2.6 Office of Intelligence and Analysis

This office is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States.

18.2.7 Office of Operations Coordination

This is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the department and with governors, Homeland Security advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide.

18.2.8 Federal Law Enforcement Training Center

This training center provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

18.2.9 Domestic Nuclear Detection Office

This office works to enhance the nuclear detection efforts of federal, state, territorial, tribal, and local governments and the private sector and to ensure a coordinated response to such threats.

18.2.10 Transportation Security Administration

The Transportation Security Administration protects the nation's transportation systems to ensure freedom of movement for people and commerce.

18.2.11 United States Customs and Border Protection

The Customs and Board Protection is responsible for protecting our nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.

18.2.12 United States Citizenship and Immigration Services

This department is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities.

18.2.13 United States Immigration and Customs Enforcement (ICE)

ICE, the largest investigative arm of the DHS, is responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation, and infrastructure security.

18.2.14 United States Coast Guard

The Coast Guard protects the public, the environment, and U.S. economic interests—in the nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security.

18.2.15 Federal Emergency Management Agency

The Federal Emergency Management Agency prepares the nation for hazards, manages federal response and recovery efforts after any national incident, and administers the National Flood Insurance Program.

18.2.16 United States Secret Service

The Secret Service protects the president and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud, and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.

18.2.17 Office of the Secretary

This entity oversees activities with other federal, state, local, and private entities as part of a collaborative effort to strengthen our borders, provide for intelligence analysis and infrastructure protection, improve the use of science and technology to counter weapons of mass destruction, and create a comprehensive response and recovery system. The Office of the Secretary includes multiple offices that contribute to the overall Homeland Security mission.

18.2.18 Privacy Office

This office works to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while achieving the mission of the DHS.

18.2.19 Office for Civil Rights and Civil Liberties

This office provides legal and policy advice to department leadership on civil rights and civil liberties issues, investigates and resolves complaints, and provides leadership to Equal Employment Opportunity Programs.

18.2.20 Office of Inspector General

This office is responsible for conducting and supervising audits, investigations, and inspections relating to the programs and operations of the department, recommending ways for the department to carry out its responsibilities in the most effective, efficient, and economical manner possible.

18.2.21 Citizenship and Immigration Services Ombudsman

This provides recommendations for resolving individual and employer problems with the United States Citizenship and Immigration Services in order to ensure national security and the integrity of the legal immigration system, increase efficiencies in administering citizenship and immigration services, and improve customer service.

18.2.22 Office of Legislative Affairs

This office serves as primary liaison to members of Congress and their staffs, to the White House and executive branch, and to other federal agencies and governmental entities that have roles in assuring national security including the following:

- Office of the General Counsel
- Office of Counternarcotics Enforcement
- Office of Public Affairs
- Executive Secretariat
- Military Advisor's Office

18.2.23 Homeland Security Advisory Council

The Homeland Security Advisory Council provides advice and recommendations to the secretary on matters related to homeland security. The council comprises leaders from state and local government, first responder communities, the private sector, and academia.

18.2.24 National Infrastructure Advisory Council

The National Infrastructure Advisory Council provides advice to the secretary of Homeland Security and the president on the security of information systems for the public and private institutions that constitute the critical infrastructure of our nation's economy.

18.2.25 Homeland Security Science and Technology Advisory Committee

The Homeland Security Science and Technology Advisory Committee serves as a source of independent, scientific, and technical planning advice for the undersecretary for Science and Technology.

18.2.26 Critical Infrastructure Partnership Advisory Council

The Critical Infrastructure Partnership Advisory Council was established to encourage effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments.

18.2.27 Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities

The Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities was established to ensure that the federal government appropriately supports safety and security for individuals with disabilities in disaster situations.

PART VI
Legislation and Regulations

CHAPTER 19 Government Laws
CHAPTER 20 Government and HIPAA
CHAPTER 21 National Industrial Security Program (NISP)
CHAPTER 22 Sensitive but Unclassified (SBU) Information Control Procedures
CHAPTER 23 Operation Security: A Law Enforcement Concern
CHAPTER 24 Camera Surveillance
CHAPTER 25 Eavesdropping Threats and IP Phone Systems
CHAPTER 26 Facility Security

19
Government Laws

The information in this chapter may be challenging, but reading and understanding some of the many laws that govern information security will help anyone who deals with sensitive information.

Following are a few of the more important federal laws governing information security. At the end of each passage is a review. Yes, the reading is dry, but it is important, and it is well worth the effort in order to increase your knowledge of what is legal and what is not.

19.1 Economic Espionage Act of 1996

According to The Computer Security Institute, the "theft of proprietary (including intellectual and confidential trade secret) information is perhaps the greatest threat to United States' economic competitiveness in the global marketplace." Before the passage of the Economic Espionage Act of 1996, it was difficult prosecuting trade secret cases within federal statutes that dealt with stolen property, mail, and wire fraud.

Certain conditions had to be met in order to prosecute espionage cases under U.S. Code Title 18 Crimes and Criminal Procedures, Chapter 37 Espionage and Censorship. For example, the stolen/lost/compromised information had to be national defense related and one needed to prove that the information was intended to or could have resulted in losses and injury to the United States. Congress soon realized that nongovernment intellectual property or trade secrets could play an increasingly important role in the national economy and introduced The Economic Espionage Act of 1996.

19.1.1 Defining Trade Secret

The Economic Espionage Act of 1996 defines the term *trade secret* as

> … all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and regardless of how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.
>
> It stipulates if … the owner thereof has taken reasonable measures to keep such information secret, and; the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public, that the owner of a trade secret is the person or entity that has rightful legal or equitable title to or license in, the trade secret—meaning that owner determines the trade secret. Despite the definition provided in the Act, once a case makes it to court, proving that something is a trade secret will be difficult if it was not properly marked and protected under lock and key.

19.1.2 Two Provisions

The act contains two separate provisions that make the theft or misappropriation of trade secrets a federal criminal offense. The first provision is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, any instrument of a foreign government, or foreign agent. In contrast, the second provision makes the commercial theft of trade secrets a criminal act regardless of who benefits.

19.1.2.1 Foreign Economic Espionage The first provision under Section 1831 is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, any instrument of a foreign government, or a foreign agent.

19.1.2.2 Commercial Theft The second provision under Section 1832 makes the commercial theft of trade secrets a criminal act regardless of who benefits.

19.1.3 Penalties

A violation of Section 1832 can result in stiff criminal penalties. A person who commits an offense in violation of Section 1832 can be

imprisoned up to 10 years and fined up to $500,000. A corporation or other organization can be fined up to $5,000,000. If the trade secret theft benefits a foreign government, foreign instrumentality, or foreign agent, the penalties are even greater.

Section 1831 provides that a person can be imprisoned up to 15 years and fined up to $500,000 if the offense is committed "intending or knowing" that the offense will "benefit a foreign government, foreign instrumentality or foreign agent." A corporation or other organization can be fined up to $10,000,000.

19.1.4 Protecting Trade Secrets

Because the world is a shrinking place and globalization and technology make it possible to do business anywhere in the world, it has become difficult for companies to protect their trade secrets. A mobile work force, employee turnover, the Internet, wireless computing, e-mail, and cell phones increase the many ways in which trade secrets can be stolen. Companies that grow at a fast pace have difficulty putting in place formal structure and procedures that are necessary to protect trade secrets. Worse, if their trade secrets are stolen, the methods in which the trade secrets were lost or stolen may never be detected. According to the American Society for Industrial Security, in 1999, Fortune 1000 companies sustained losses of more than $45 billion from thefts of their proprietary information (ZDNET, 2000). Competitors gain access to proprietary information from a number of ways including

- Illegal hacking/unauthorized access to a company's computers
- Social engineering
- Corporate spies
- Disgruntled employees

Companies protect their information by installing firewalls, computer security measures, strong information protection policies, and effective employee training. Nondisclosure agreements should be executed between the company and all employees, vendors, clients, partners, and anyone else who will have access to proprietary information or potential trade secrets. Policies and procedures need to be in place that state specifically how proprietary information is to be handled and protected.

They should also be trained in the various methods by which information is stolen and how to recognize and respond to such attempts.

19.1.5 Limitations

Here is the most critical element of the act—a defendant cannot be convicted if it is proven that elements of a trade secret were discovered through parallel development or reverse engineering. The act does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skills, or abilities. The act also does not prohibit legitimate economic collection or reporting by personnel of foreign governments by lawful means. In essence, if the owner of the proprietary information or trade secret did not take reasonable measures to lock it down and it is proven that the trade secrets were not properly protected, the case may be nearly impossible to prosecute.

19.1.6 Gillette® and Kodak® Cases

Some of the most notable economic espionage cases successfully tried under the act include those of a new Gillette razor design, the Avery Dennison Corporation, and the Eastman Kodak Corporation, which are detailed in a classified espionage database maintained by the Defense Personnel Security Research Center.

The center gives this description of the Gillette and Kodak cases:

- Steven Louis Davis was indicted in Tennessee on October 3, 1997, on five counts of fraud by wire and theft of trade secrets for stealing and disclosing trade secrets on a new shaving system by The Gillette Company. Davis was employed by Wright Industries, subcontracted to assist Gillette in the project. Davis is alleged to have sent confidential engineering drawings for the new Gillette razor to Gillette's competitors, including Warner-Lambert, Bic, and American Safety Razor Co., and possibly to a foreign-owned company.
- Harold C. Worden was a 30-year employee of the Eastman Kodak Corporation who established his own consulting firm upon retiring from Kodak—allegedly brokered the consulting services of more than 60 other Kodak retirees, some of whom

consulted for competitors and foreign firms. During his time at Kodak, Worden was project manager for the now 401 machine, a new machine designed to inexpensively produce the clear plastic base used in consumer film. When Worden retired, he took with him thousands of documents marked "confidential" about the development of the 401 machine, and he recruited his successor to continue providing confidential information. Worden allegedly removed numerous drawings, plans, and manuals and that resulted in possibly billions-of-dollar losses to Eastman Kodak Corp.

Bibliography

Annual report to Congress on foreign economic collection and industrial espionage. (1997, June). *National Counterintelligence Center*.

Cornell Law School Web Library. Retrieved from http://www4.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18.html.

Espionage Act of 1996. Retrieved from http://rf-web.tamu.edu/security/secguide/T1threat/Legal.htm.

The Economic Espionage Act of 1996: A Brief Guide. *National Counterintelligence Center*.

Unclassified espionage database. Defense Personnel Security Research Center. Retrieved from http://rf-web.tamu.edu/security/secguide/Spystory/Industry.htm.

ZDNET. (2000, September 11). The untold tally of "Netspionage." Retrieved from http://news.zdnet.com/2100-9595_22-523790.html.

20
Government and HIPAA

20.1 SSI-Related Laws and Terminology

SSI has implications in many areas, including access to information, the privacy of electronic data and computers, and trade secrets. Keeping certain information private or secure while allowing people to have as much access as possible is a difficult balance. The laws of this country attempt to do just that. (The listing of any website below does not constitute endorsement.)

20.2 Access to Information

Several federal laws in the United States apply to access of information. These laws cover who can access information and what information people can legally obtain in certain circumstances. Each of these laws applies to a particular type of information or reason for access. The four important laws are the Freedom of Information Act (FOIA), the Privacy Act of 1974, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The federal government provides much information to the public about these laws. Anyone can visit the U.S. Department of Justice's website (http://www.doj.gov) to read the text of the laws and summaries and analyses of the laws and what citizens' rights under the laws are, including how to access information and protect their personal information. This department of the federal government serves a variety of functions that seek to preserve justice and enforce the laws. Under President George W. Bush, the department received a new focus: fighting terrorism.

The sections below each focus on one of the above laws.

20.2.1 FOIA

According to the U.S. Department of Justice's guide to the FOIA, "the FOIA (5 U.S.C. § 552) generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions" (http://www.usdoj.gov/oip/introduc.htm). The guide includes the entities that the FOIA applies to, how to make requests under the FOIA, fees, the exemptions from the FOIA, and references to other materials about the FOIA.

The website of the U.S. Department of Justice contains all of this information. See http://www.usdoj.gov/oip/foi-act.htm. The Chicago Public Library also has a good website that explains the FOIA. See http://chipublib.org/008subject/006govinfo/foia.html.

Many agencies are subject to the FOIA and provide information on their websites that tells how to access information from them. For example, see http://foia.fbi.gov/ for the FBI's FOIA web page.

20.2.2 The Privacy Act of 1974

The Privacy Act of 1974 (5 U.S.C. § 552a) overlaps somewhat with the FOIA, but its main function is to allow personal access to an individual's own records. This act addresses the privacy of information held by agencies and the remedies for violation of privacy. Once again, the U.S. Department of Justice has a wealth of information on its website about the Privacy Act of 1974.

The text of the act can be found online at http://www.usdoj.gov/oip/privstat.htm, and an overview of the 2004 edition of the act as well at http://www.usdoj.gov/oip/1974indrigacc.htm.

20.2.3 The PATRIOT Act

Just as the U.S. Department of Justice has much information about the FOIA, it also clearly describes the PATRIOT Act and how it

fights terrorism. The U.S. Department of Justice tries to dispel what it calls *misconceptions* about the act. Congress passed the act in the wake of the terrorist attacks of September 11, 2001, and amid bipartisan support, Congress passed the U.S.A. Patriot Improvement and Reauthorization Act of 2005 on March 2, 2006.

The PATRIOT Act has been the subject of controversy, and some civil liberties organizations claim that it has gone too far in invading the privacy of citizens under the auspices of protecting against terrorism. For more reading about the opposition to the PATRIOT Act, see the following links:

- A Guide to the PATRIOT Act, Part One—http://www.slate.com/id/2087984/
- The Electronic Frontier Foundation web page on the Patriot Act—http://www.eff.org/patriot/
- The American Civil Liberties Union website on the Patriot Act—http://www.aclu.org/safefree/resources/17343res20031114.html

20.3 Privacy of Electronic Data and Computers

Another issue with SSI is the security of information that is sent by or stored on computers. E-mail and online bill paying are just two of the many useful applications of modern technology that can be vulnerable to spying or theft of information. To preserve freedom and access to information while also protecting the privacy rights of people, many organizations exist that also seek to educate the average citizen about privacy issues. The websites of these groups are particularly helpful for learning what the important issues are in Internet privacy and how to protect personal information online. See below.

20.3.1 Center for Democracy and Technology

The Center for Democracy and Technology, which is a nonprofit organization that seeks to preserve free expression on the global Internet, has a guide to online privacy and access to information. Visit their website at http://www.cdt.org/privacy/guide/start/.

Along with the guide, the website of this organization has much to offer. See http://www.cdt.org/. The site has the latest news in Internet privacy issues, laws and proposed laws, reports and articles, and a resource library.

20.3.2 Computer Crime and Intellectual Property Section (CCIPS)

The CCIPS of the U.S. Department of Justice works to carry out the U.S. Department of Justice's plans and programs related to computer and intellectual property crimes. The CCIPS not only tries to prevent computer crimes but also prosecutes cases. The website (http://www.cybercrime.gov/) has pages for computer crime, intellectual property, electronic evidence, and other high-tech legal issues. These pages address the latest news, cases, and laws, and explain just what computer crimes and intellectual property are.

20.3.3 Information Security and Privacy Advisory Board (ISPAB)

Congress created the ISPAB after passing the Computer Security Act of 1987. (See the end of this section for more information about the act.) One function of the board is to advise the NIST, which is a federal agency, about privacy and information security issues that are relevant to the federal government's information systems. The ISPAB's website is http://csrc.nist.gov/ispab/. This website explains what the ISPAB does and has links to the board's annual reports and recommendations. Unfortunately, the most recent annual report on the site is from 1995.

20.4 Cryptology

20.4.1 National Security Agency (NSA)

The NSA is the U.S. government agency responsible for cryptography, which includes protecting the government's information systems and understanding foreign information by use of SIGINT. Visit the NSA's website at http://www.nsa.gov/ for more information about how it uses cryptology.

20.4.2 Computer Security Resource Center (CSRC)

CSRC provides information about cryptographic standards and application, security research and emerging technologies, viruses, and other security issues related to computers. The information about encryption applies to federal agencies and explains how using encryption can help keep certain information secure. The Cryptographic Toolkit offers guidance but does not give the actual software for implementation. Although most of the information on the CSRC's website pertains to federal agencies, it does offer some tips for small businesses. The CSRC's website seems to be geared to users who already have an understanding of encryption and security rather than those who are unfamiliar with these issues. See http://csrc.nist.gov/index.html.

20.4.3 Computer Professionals for Social Responsibility

The Computer Professionals for Social Responsibility organization has a website that offers information about intellectual property, global privacy, and civil liberties issues related to computers. See https://www.cpsr.org/issues/privacy. Founded in the United States, this organization advocates responsible use of computers and does so primarily by educating the public and policymakers.

20.4.4 Electronic Frontier Foundation (EFF)

The EFF is a nonprofit organization that strives to protect what it refers to as digital rights, which includes telephones, computers, and the Internet, music, television, and movies review. See http://www.eff.org/. The EFF is an advocate for free speech and privacy issues, and its website also has the latest news about laws and cases in this realm. Topics addressed on its website include fair use, intellectual property, bloggers' rights, and file sharing.

20.4.5 Electronic Privacy Information Center (EPIC)

The EPIC has an especially useful website. See http://www.epic.org for privacy-related information. The EPIC website offers

comprehensive coverage of privacy issues and has information on domestic surveillance, the FOIA, the PATRIOT Act, telephone records, bill tracking, and much more. EPIC is well respected and has received praise from *The Wall Street Journal*, *Christian Science Monitor*, and the *American Bar Association Journal*. The EPIC website also has a good deal of information about medical privacy, including HIPAA. See http://www.epic.org/privacy/medical/.

EPIC also has a joint project with Privacy International, which is a human rights group based in London, England, called Privacy.org. The website http://www.privacy.org offers news that is updated daily and other information about privacy.

20.5 Privacy Laws

Since the development of the Internet, Congress has passed several laws governing privacy and use of the Internet. See below.

20.5.1 National Information Infrastructure Protection Act of 1996

For the text of the National Information Infrastructure Protection Act of 1996, see the website at http://www.usdoj.gov/criminal/cybercrime/1030_new.html. For analysis of the act, see http://www.justice.gov/criminal/cybercrime/1030_anal.html. This act amends the Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030).

20.5.2 Computer Security Act of 1987

15 U.S.C. §§ 271 et seq. (Public Law 100-235), Computer Security Act of 1987 improves the security of federal computer systems. See http://www.fas.org/irp/offdocs/laws/pl100235.htm.

20.6 Trade Secrets

Another kind of sensitive information is a trade secret. Sometimes, companies have information, perhaps a formula or design that is unique to their company or product and is confidential. Although trade secrets share certain characteristics with patents and trademarks,

trade secrets are separate from both of these. For more information, see these websites:

- About.com at http://inventors.about.com/od/tradesecrets
- Free Advice at http://www.freeadvice.com (click on "Intellectual Property," and go to "Trade Secrets" from there)
- Nolo at http://www.nolo.com (under "patents, copyright & art," click on "trade secrets")
- Findlaw (http://www.findlaw.com)

Laws applying to trade secrets are the Uniform Trade Secrets Act and the Economic Espionage Act.

20.6.1 Uniform Trade Secrets Act

For the text of the act, see the website at http://www.law.upenn.edu/bll/ulc/fnact99/1980s/. This act is a model act that many, but not all, states have chosen to adopt as part of their state law.

20.6.2 Economic Espionage Act

Visit http://www.usdoj.gov/criminal/cybercrime/eea.html for prosecutions, legislative history, and information about intellectual property. The text of the law is at the NSI website (http://nsi.org/Library/Espionage/usta.htm).

Companies sometimes keep information secret that could harm the public. For example, Bill Moyers of the Public Broadcasting System researched chemicals and the health effects from exposure to them. When companies conceal the danger of the materials they use, the effects might harm and perhaps even lead to the death of the people exposed. See http://www.pbs.org/tradesecrets. The Emergency Planning and Community Right-to-Know Act applies to toxic chemicals and requires reporting on certain chemicals to make the public aware of potential risks. Citizens of the United States have a legally defined right to know about certain chemicals, and this information can no longer be kept secret. See http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/epcraOverview.htm.

20.6.3 Coca-Cola® Case

The most famous trade secret case in recent history is the Coca-Cola case. In federal court, three people have been charged with conspiring to steal new product samples of Coca-Cola and attempting to sell them to rival PepsiCo, Inc. For more information about the case, read these stories at MSNBC.com:

- "Trio indicted in Coca-Cola trade secret case" (http://www.msnbc.msn.com/id/13818266)
- "Coca-Cola espionage case to go to trial" (http://www.msnbc.msn.com/id/15050780/)
- "Coca-Cola trade secrets theft case set for trial" (http://www.msnbc.msn.com/id/15209024/)
- "Two admit plotting to steal Coke secrets" (http://www.msnbc.msn.com/id/15401600/)

21

National Industrial Security Program (NISP)

This chapter contains a summary of the NISP, retrieved from the Defense Security Service Academy at https://dssaots.dss.mil/eismpdf/eism.pdf. The entire text of the National Industrial Security Program Operating Manual (NISPOM) can be viewed online at http://www.dtic.mil/whs/directives/corres/html/522022m.htm.

21.1 NISP Overview

When one stops to consider that nearly 90% of all U.S. classified information originates within the industrial environment, the impact of industry on the national security can scarcely be overemphasized.

21.1.1 A Partnership

The NISP is a partnership between the federal government and private industry to safeguard classified information. As a Facility Security Officer (FSO), you will be required to ensure that your firm adheres to the policies, practices, and procedures of the NISP. So it is essential that you have a clear understanding of the overall organization, mission, and functions of the NISP, as well as those of the Defense Security Service (DSS), which oversees the NISP for the Department of Defense and works with you, the FSO, in carrying out your duties.

21.1.2 The Government–Industry Relationship

The government, especially the military, has a great and pressing need for state-of-the-art technology: weapons systems, information technology, communications systems, and so forth. With rare exceptions,

the government does not research, develop, or manufacture these items. Instead, it relies on industry. It also relies on industry for ordinary supplies and support services that, in some cases, require access to areas containing classified information. In order for industry to meet the government's need, it must have access to classified information. This is where the NISP comes in.

21.1.3 Purpose of the NISP

The NISP is a government–industry team program to safeguard classified information entrusted to industry. The government sets requirements for the protection of classified information in the hands of industry, and industry implements these requirements with government advice, assistance, and oversight. Four federal agencies, the Cognizant Security Agencies (CSA), provide these services:

- Department of Defense (DOD)
- Department of Energy (DOE)
- Nuclear Regulatory Commission (NRC)
- Central Intelligence Agency (CIA)

The DOD has delegated the security oversight and the administration of its classified activities and contracts to the DSS. For most security matters, you will be dealing directly with two elements of DSS: the Defense Industrial Security Clearance Office and the DSS Field Office for your area. More discussion on this topic is to follow.

21.2 Classified Information

Protection of classified information is what the NISP is all about. You need to understand what classified information is so that you can fulfill your duties as an FSO in protecting that information and instructing others in its protection. Classified information is official government information which has been determined to require protection against unauthorized disclosure in the interest of national security and which has been so identified by being marked *top secret*, *secret*, or *confidential*. These three categories pervade all aspects of the NISP. They form the

basis for the handling and safeguarding requirements for classified information. All facilities and all cleared personnel within the NISP are cleared at one of these levels. The classification categories are as follows.

21.2.1 Classified

It is classified information or material that requires protection, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security that the original classification authority is able to identify or describe. An example of damage would be the compromise of information that indicates the strength of our armed forces, or disclosure of technical information about our weapons, such as performance characteristics, test data, design, and production data.

21.2.2 Secret

It is classified information or material that requires a substantial degree of protection, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. Wrongful disclosure of secret information could lead to a disruption of foreign relations significantly affecting national security; could significantly impair a program or policy directly related to national security; could reveal significant military plans or intelligence operations; or could compromise significant scientific or technological development relating to national security.

21.2.3 Top Secret

It is classified information that requires the highest degree of protection, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to our national security that the original classification authority is able to identify or describe. Wrongful disclosure of top secret information could lead to war against our nation or its allies; could disrupt vital relations with other countries; could compromise our vital defense plans or our

cryptographic and communications intelligence systems; could reveal sensitive intelligence operations; or could jeopardize a vital advantage in an area of science or technology.

Always be aware that unauthorized disclosure of any classified information can cause damage to the national security. Do not fall into the trap of thinking of some classified information as only confidential. Different degrees of safeguarding are required for the three levels, but all three types of information must be protected.

21.3 Components of the NISP (DOD)

For DOD, the NISP has four main components:

- User agencies, in the role of Government Contracting Activities (GCA)
- Cleared contractors
- DSS, in the role of the Cognizant Security Office (CSO)
- CSO on behalf of the DOD, which is the CSA

21.3.1 User Agencies

A facility becomes a part of the NISP at the request of a user agency or of a cleared contractor to a user agency. A user agency is a federal agency that has entered into an agreement with the secretary of defense, the executive agent for the NISP, for industrial security services. The user agencies are government customers of private industry. The Air Force, the Army, the Navy, in fact, all DOD components are user agencies. There are also 24 non-DOD departments and agencies that are user agencies.

Each user agency has one or more GCAs. A GCA is an element of a federal department or agency that is designated to handle acquisitions for that department or agency. Experts at GCAs of the user agencies determine when one of their contracts will involve classified information. They then identify in the contract the kinds of classified information to which the contractor will require access. If the contractor will be generating material or information that is classified, the GCA will provide guidance to the contractor (incorporated in the contract) as to what information is classified and at

which level. Note that the user agency, not the contractor, owns the classified information.

The DOE, NRC, and CIA each have procedures for oversight and administration of the NISP for contracts involving these agencies. Those procedures are not covered in this book.

The following are user agencies under the NISP:

- Department of Defense
- Department of State
- Department of Commerce
- Department of Treasury
- Department of Transportation
- Department of the Interior
- Department of Justice
- Department of Agriculture
- Department of Labor
- Federal Reserve System
- General Services Administration
- Small Business Administration
- U.S. Trade Representative
- U.S. International Trade Commission
- National Science Foundation
- Environmental Protection Agency
- General Accounting Office
- Federal Emergency Management Agency
- National Aeronautics and Space Administration
- U.S. Arms Control & Disarmament Agency
- U.S. Agency for International Development
- Nuclear Regulatory Commission
- Department of Health and Human Services
- Department of Education
- Cleared Contractors

All work performed by industry for the U.S. government is performed under contract. If classified work or products are involved, it is necessary to clear the contractor (the private industrial firm involved). This clearance, called a Facility Security Clearance (FCL), is an administrative determination made by the government that the facility is eligible for access to classified information.

21.3.2 Cleared Contractors

There are about 11,000 cleared contractors in the NISP, ranging in size from industrial giants such as Boeing, Northrop Grumman, and Lockheed Martin to the many smaller firms and one-person businesses. About half of all cleared contractors possess classified material at their own facilities. The other half, most of whom are service organizations, do not possess classified material. Instead, their employees have access to classified information at the possessing facilities or at user agency installation locations.

Cleared contractors employ 800,000 cleared employees. There are more than 11 million classified documents entrusted to cleared contractors. So far, we have seen that there is a mutually beneficial relationship between government and industry. The government receives essential goods and services, and industry profits from the exchange. User agencies are federal government agencies that need goods and services involving classified information, and industrial firms become cleared contractors as a result of that need. Let us turn now to the third component of the NISP for DOD: the DSS. We said that the DOD has delegated security administration of its classified activities and contracts to DSS. In this role, DSS is sometimes referred to as the CSO within the DOD. By their agreements with the secretary of defense, the heads of the other user agencies authorize DSS to administer the security measures for their classified activities and contracts. How did the DSS come to play this important role?

21.3.3 Defense Security Service

For many years, until around the time of the Korean War, the agencies that are now the user agencies administered their own security programs. Then, to provide greater uniformity in the handling of classified information, the Defense Industrial Security Program (DISP) was formed. The uniformity simplified the handling of classified information for industry. Rather than having to comply with separate security rules and regulations set by each government agency for each contract, there was only one set of rules for all contracts awarded within the DISP. To achieve even greater uniformity in the security requirements for classified contracts, the NISP was launched in 1993.

Now the DOE, the NRC, and the CIA have joined with the DOD in subscribing to a single set of rules for their classified contracts: the NISPOM.

The administration of the DISP was undertaken initially by the individual military services. In 1965, the DISP was placed under the centralized management of the Defense Logistics Agency (DLA). The Defense Investigative Service was established in 1972 and, in 1980, replaced DLA as the administrative agency for the DISP. With the creation of the NISP in 1993, the secretary of defense designated the DIS as the CSO for DOD. In 1997, DIS was renamed the Defense Security Service. The director, DSS, administers the NISP on behalf of the secretary of defense and the user agencies.

21.3.4 Facility Security Office Role

We now have the four components of the NISP for DOD: user agencies, cleared contractors, and the DSS. An FSO for a cleared contractor in the NISP has the main duty of ensuring that his or her facility abides by the terms of the Security Agreement DD Form 441 (Department of Defense Security Agreement that is a legal and binding agreement with the government, which outlines the terms for safeguarding classified information). This duty involves the oversight of security practices at your facility and cooperation with DSS in maintaining a viable security program. A security program is more than just a matter of physically protecting information. Anyone who works at a non-possessing facility still has security requirements to be met at the facility. These requirements apply equally to all types of facilities. One of the most important aspects of an FSO's job will be to educate all cleared personnel about their security responsibilities.

21.4 The FSO and the Industrial Security Representative (IS REP)

An FSO's point of contact with DSS is the IS REP. The IS REP serves as a representative of the U.S. government in those matters of industrial security covered by the NISP. The IS REP does not function as a police officer. The IS REP is assigned to work with facilities in developing and maintaining security programs.

The FSO will most commonly see an IS REP in one of these situations:

- During an initial survey when a new facility is being processed for a security clearance
- When necessary to provide advice and assistance
- When performing a scheduled security review
- Structure of DSS: Industrial Security

21.5 Structure of DSS: Industrial Security

The DSS Headquarters is presently located in Alexandria, Virginia. Its mission is accomplished through the efforts of highly skilled personnel assigned to field offices located throughout the United States. Each IS REP is assigned to a field office.

Each field office is managed by a Field Office Chief. There is a Deputy Field Director who oversees the operation of all field offices within each of five geographical areas.

The services of a DSS Information Systems Security Professional and a Counterintelligence Specialist are available to each field office. The DSS Office of Security Services International provides support to cleared contractor employees at overseas locations.

Visit the DSS website www.dss.mil and click on About DSS to see more detailed information regarding the organization and location of DSS Offices.

22

Sensitive but Unclassified (SBU) Information Control Procedures

22.1 Policies to Control SBU Information

The history through 2002 of using the label SBU was described in detail in Congressional Research Service (CRS) Report RL31845 and is summarized briefly in this section, which also updates action through February 15, 2006.

22.1.1 Introduction to the Term SBU

Federal agencies began to use the term SBU in the 1970s, but the term has never been defined in statutory law. Starting in 1987 and continuing today, when using the term *sensitive information*, some agencies refer to the definition for sensitive information that was used in the Computer Security Act of 1987, Public Law (P.L.) 100-235, and to information exempt from disclosure in the FOIA and the Privacy Act, as amended.

22.1.2 Computer Security Act Definition of Sensitive

The Computer Security Act of 1987 (CSA) was intended to protect the security and privacy of sensitive unclassified information in federal computer systems and the systems themselves. P.L. 100-235 defined the term *sensitive* information as

> any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct

> of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 3).

Because P.L. 100-235 applied to *sensitive information* that was not classified, some say it defined *sensitive but unclassified*. Pursuant to the CSA, federal agencies were responsible for protecting such sensitive information and for developing plans to secure it "commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information being protected." The CSA, among other things, required agencies to develop security plans for systems containing sensitive information. It authorized the National Bureau of Standards (NBS), now called the NIST, to create a security-oriented standards program. The definition of *sensitive information* was placed within the section that listed NBS's functions, and subsequently, NIST became responsible when the agency's name was changed in 1988. In 1992, NIST issued guidance giving agencies authority to implement risk-based procedures to protect sensitive information pursuant to P.L. 100-235. NIST reiterated that "interpretation of the CSA's definition of sensitive is, ultimately, an agency responsibility." It identified three security goals.

Typically, protecting sensitive information means providing for one or more of the following: Confidentiality—disclosure of the information must be restricted to designated parties; Integrity—the information must be protected from errors or unauthorized modification; and Availability—the information must be available within some given time frame (i.e., protected against destruction).

Although it was not mandatory, NIST urged agency information owners to use a risk-based approach to identify information to be protected and controls needed based on risk of loss: The type and amount of protection needed depends on the nature of the information and the environment in which it is processed. The controls to be used will depend on the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in the system.

22.1.3 SBU in Relation to the FOIA

Predating the CSA, the FOIA was enacted to ensure public access to certain types of information held by federal agencies. However, it permits agencies to exempt from public disclosure nine types of information:

1. Information classified in the interest of national defense or foreign policy
2. Internal personnel rules and practices of an agency
3. Information specifically exempted from disclosure by statute
4. Trade secrets and commercial or financial information obtained from a person and privileged or confidential
5. Interagency or intra-agency memoranda or letters reflecting predecision attitudes
6. Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy
7. Specified types of law enforcement records or information
8. Financial institution regulation or supervision reports
9. Geological and geophysical information and data concerning wells

The CSA, the report accompanying it, and NIST guidance included explicit instructions that categorizing information as *sensitive* did not confer authority to withhold information sought pursuant to Section 552 of Title 5 United States Code (FOIA). Nevertheless, as will be discussed below, some federal agencies say that all information categorized as For Official Use Only (FOUO) or in related categories is SBU, or that all SBU information may be withheld under FOIA.

22.1.4 Department of Justice Broadens Interpretation of Exemptions from FOIA

After the terrorist attacks of September 2001, the White House and the Department of Justice, in a series of administrative actions, expanded agencies' ability to withhold SBU information. To prevent potential use of sensitive information by terrorists, in March 2002, the White House issued the so-called Card memo, which required agencies to examine their information holdings and policies; withhold

information, including SBU information; and use FOIA exemptions if there was a sound legal basis to do so. Attorney General John Ashcroft's prior memorandum of October 2001 on this issue was referenced. These statements modified the Clinton administration's policy, which urged agencies to release information if there was no foreseeable harm in doing so.

Subsequently in 2003, the Department of Justice issued guidance based on court decisions that broadened interpretation of exemptions from disclosure under FOIA. It also discussed the new exemption 3 provision of P.L. 107-296, the Homeland Security Act of 2002, which protects voluntarily submitted critical infrastructure information. The Freedom of Information Act Guide, 2004, explained how an agency's ability to restrict the release of sensitive information via FOIA would be broadened and, citing the September 11, 2001, attacks, the passage of P.L. 107-296 and the creation of the DHS cautioned vigilance on releasing sensitive information.

These changes have greatly impacted many aspects of the operation of the federal government, including the administration of the FOIA. Much greater emphasis is now placed on the protection of information that could expose the nation's critical infrastructure, military, government, and citizenry to an increased risk of attack. As a result of these changes, federal departments and agencies should carefully consider the sensitivity of any information the disclosure of which could reasonably be expected to cause national security harm.

The guide reiterated, however, that use of labels such as SBU, Sensitive Homeland Security Information (SHSI), and so forth does not "provide for any protection from disclosure under any (FOIA) exemption …" (except for Critical Infrastructure Information [CII], which is protected by statute). Nevertheless, the guide encouraged agencies to exempt from disclosure information labeled *SHSI* or other nonclassified information that is highly sensitive, as referenced in the aforementioned court decisions and in Homeland Security Presidential Directive HSPD-7, issued on December 22, 2003:

> Whatever the safeguarding label that an agency might (or might not) use for the information maintained by it that has special sensitivity—e.g., "for official use only" (FOUO), "restricted data" (a Department of Energy designation), or "Sensitive Homeland Security Information"

(SHSI)—whenever predominantly internal agency records may reveal information the disclosure of which could reasonably be expected to cause any of the harms described above [to critical systems, facilities, stockpiles, and other assets], responsible federal officials should carefully consider the propriety of protecting such information under Exemption 2.

22.2 Policies to Protect Specific Types of Sensitive Information Involving Scientific and Technical Applications

Specific laws have been enacted and policies and procedures are in varying stages of implementation that define and protect sensitive unclassified science- and technology-related information in such fields as critical infrastructure, transportation, environmental impacts, biology, geospatial data, and DHS information. These laws and their criticisms have been summarized in the next section.

The need to protect critical infrastructure information is based on the premise that potential terrorists should not have access to information that might expose vulnerabilities in, or provide roadmaps to, the nation's core physical transportation, water, communication, energy, and related systems, or to major buildings, bridges, and other types of major structures.

22.2.1 Vulnerabilities

As an example of critical infrastructure vulnerabilities, Charlie Reeder, Interagency Operations Security Support Staff, DOD, and part of a Pentagon group that represents the NSA, CIA, General Services Administration, and DOE, is reported to have said that "… he's seen government websites include maps of installations … specifications of weapons and communications systems … and much more…. When we publish this information on the Internet, we might as well fax it directly to our adversaries…." He also commented that "According to a message sent by Secretary of Defense Donald Rumsfeld … an al Qaeda training manual recovered in Afghanistan states using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy." Open-source information can be accessed through Internet sites, job announcements, budget documents, and newsletters. Similarly, a

survey by Computerworld noted that "the widespread availability of sensitive information on corporate websites appears to have been largely overlooked by IT and security managers…." Among the information available on the web are "3-D models of the exterior and limited portions of the interior of the Citigroup headquarters building in Manhattan—one of the sites especially named in the latest terror advisory issued by the Department of Homeland Security," and various similar kinds of information about the building's structural design weaknesses.

22.2.2 Critical Infrastructure Information Act of 2002

In part to cope with issues like these, the Critical Infrastructure Information Act of 2002, Title II of P.L. 107-296, prohibits disclosure under FOIA of "critical infrastructure information" relating to the security of critical infrastructure and protected systems submitted to DHS voluntarily by private companies. Criminal penalties for disclosure by employees under this statute include fines, dismissal, or imprisonment for up to a year (Section 214.96). The statute also provides for the preemption of state freedom of information laws regarding the public disclosure of such information if it is shared with a state or local government official in the course of DHS's activities.

22.2.3 DOD and DHS Rules

The DOD issued a memo on March 25, 2003, that applied prohibitions like those in P.L. 107-296 to critical infrastructure information voluntarily submitted to DOD. On April 15, 2003, DHS published interim rules to implement the critical information infrastructure protection provisions of P.L. 107-296, which would extend the rules to other agencies by requiring them to pass to DHS similar information that they receive.

22.2.4 Homeland Security Presidential Directive 7

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which among other things, directed all federal agencies to protect voluntarily submitted information

about critical infrastructure vulnerabilities in line with Title II of P.L. 107-296.

22.2.5 Protected Infrastructure Information Program

The DHS published an interim final rule that established the Protected Infrastructure Information Program effective February 18, 2004. It requires submitters to certify, under penalty of fine or imprisonment, that the submitted information is not subject to disclosure under the rules of another department, such as to meet health, safety, or environmental regulations. If agencies other than DHS obtain comparable information in their normal regulatory processes, the CII restrictions do not apply; if a company submitted information to DHS under the protected CII program that was identical to information required by another agency, the protection afforded to the submission to DHS would not extend to the information submitted to another agency.

This latter provision is intended to allay some of the fears that companies will submit to DHS information they do not want to be disclosed in order to hide from public information about pollution, new facilities, or security gaps. CII information submitted to DHS is not subject to disclosure under FOIA, under a new exemption 3 category, pursuant to section 214 of the Homeland Security Act of 2002, if it has not been made public previously. The language in P.L. 107-296 protects only CII submitted to the DHS, but the Department of Justice reports that in the future, it may be applied to submissions made to other federal agencies.

22.3 SSI Controls: Transportation

The FAA had been permitted since passage of the Air Transportation Security Act of 1974 to issue regulations to protect, and to distribute to those with a need to know, sensitive civil aviation security information that was obtained during security investigations or consisted of research and development information that would invade privacy, would reveal a trade secret or financial or commercial information, or would be detrimental to the safety of persons traveling by air. "The FAA implemented this authority by promulgating regulations,

which, among other things, established a category of information known as Sensitive Security Information (SSI). In 1997, the Department of Transportation (DOT) definition of SSI included 'records and information … obtained or developed during security activities or research and development activities.'" Subsequently, this type of information was given a statutory basis pursuant to the Aviation and Transportation Security Act, P.L. 107-71, which created the TSA and prohibited disclosure of certain kinds of information relating to transportation if the disclosure would be detrimental to the safety of passengers in transportation. P.L. 107-296 expanded this coverage to include information detrimental to the "security of transportation."

As the FAA was moved to the TSA, first located in the DOT and then to the DHS, the SSI withholding authority appears to have been expanded to include "all transportation related activities including air and maritime cargo, trucking and freight transport, and pipelines." On May 18, 2004, the DOT and DHS jointly promulgated revised regulations that "adopt the Homeland Security Act language as the definition of SSI. In addition, the new regulations incorporate former SSI provisions, including the 16 categories of information and records that constitute SSI." SSI information is defined by statute (49 U.S.C. section 114(s)) and an implementing regulation (49 C.F.R. part 1520) as

> (1) Security programs and contingency plans … issued, established, required, received, or approved by DOT or DHS … (2) Security Directives … (3) Information Circulars … issued by DHS or DOT regarding a threat to aviation or maritime transportation … (4) Performance specifications … (5) Vulnerability assessments … (6) Security inspection or investigative information … (7) Threat information … (8) Security measures … (9) Security screening information … (10) Security training materials … (11) Identifying information of certain transportation security personnel … (12) Critical aviation or maritime infrastructure asset information … (13) Systems security information … (14) Confidential business information … (15) … Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or

directed by the DHS or DOT, including research results … (16) Other information …

This information, like CII information, was also designated as exempt from disclosure under FOIA (49 U.S.C. section 40119b(1)) under exemption 3, which permits the withholding of information protected by other statutes, has use limitations for sharing with state or local governments, and imposes criminal penalties on federal officers or employees who disclose such information.

22.4 Identifying and Handling SSI

22.4.1 Section 15.5 of Code of Federal Regulations (CFR) Title 49

According to the informational pamphlet *Securing Information, Protecting Our Nation* by the TSA, if information falls into any of the specific categories below, it is considered SSI and must be marked and protected accordingly:

- Security programs and contingency plans
- Security directives
- Information circulars
- Performance specifications
- Vulnerability assessments
- Security inspections or investigative information
- Threat information
- Security measures
- Security screening information
- Security training materials
- Identifying information of certain transportation security personnel
- Critical aviation or maritime infrastructure asset information
- Systems security information
- Confidential business information
- Research and development

This is a condensation of the 15 specifications set forth in Section 15.5 of CFR Title 49.

22.4.2 "Need to Know" Specifics

According to this Federal Regulation, SSI is only allowed to be disclosed to covered persons on a "need to know" basis, as specified in Section 15.7. The need to know specifics are further defined in Section 15.11 and include the general circumstances for determining need to know basis:

1. When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT
2. When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT
3. When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT
4. When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of federal law
5. When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements

22.4.3 The Marking of SSI

The marking of SSI also falls under 49 CFR, Part 15. Specifically, according to this Federal Regulation:

> "(a) … In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of
>
> (1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;
>
> (2) Any title page; and
>
> (3) Each page of the document.

(b) Protective marking. The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) Distribution limitation statement. The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a 'need to know,' as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."

(d) Other types of records. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record."

22.4.4 Federal Records Act

Finally, the code specifies that destruction of SSI is subject to terms of the Federal Records Act, and that SSI must be destroyed once it is no longer needed to carry out the transportation security measure, except when state or local law states otherwise.

The TSA gives recommendations for protecting and handling SSI:

- Do not leave SSI unattended. Lock it up.
- Do not take SSI home without written permission.
- Do not discuss SSI on cell phones or other types of cordless phones, because these communications can be easily intercepted.

- SSI must be password-protected and sent as an attachment when being communicated via e-mail. Send the password separately and not in the same e-mail as the SSI.
- Protect verbal communications as you would paper or electronic formats.
- Do not entrust or discuss SSI with people who do not have a need to know.

The TSA has forms and templates for handling SSI on its website at http://www.tsa.gov/research/ssi forms.shtm.

Additionally, the TSA offers a 61-slide, basic training course on handling SSI, which can be found online at http://www.tsa.gov/assets/pdf/ssi_training.pdf.

22.4.5 Critique of SSI Rules

The ability of terrorists to capitalize on vulnerabilities in the national and foreign transportation systems in this arena has been manifested several times since 2001. Nevertheless, some critics charge that too much information is being withheld from public access. Many of the criticisms of SSI rules focus on the alleged consequences of preventing the public from accessing information that might be used to promote safety or be used in citizen oversight. For instance, some aircraft personnel and consumer advocates say that TSA's use of SSI can "muzzle debate of security initiatives and insulate TSA from criticism." The newsletter OMB Watch reported that the TSA has denied access to information when "reasonable access to it could improve safety conditions for communities and workers." Examples include TSA denying pilots access to information to comply with TSA regulations to avoid flying near nuclear power plants, disagreeing with TSA's views that information on such sites compiled from public data by the Aircraft Owners and Pilots Association should be labeled SSI and not be made available, and denying the District of Columbia government access to information to help determine if trains carrying chlorine through the District of Columbia should be rerouted. The Coalition of Journalists for Open Government (CJOG), a group of journalist advocacy organizations, in a filing on July 16, 2004, in response to regulations jointly filed by

the Department of Transportation and the Transportation Security Administration, said:

> [The] … unrestricted use of the … (SSI) designation … will have a seriously adverse impact on traditional citizen and media oversight of the governance of our seaports, airports and transit systems…. There appear to be no limits to the type of information that might be gathered or generated as SSI and then sealed. Local and state officials, bound by non-disclosure agreements, may be forced to deny access to records that state law and local ordinance require be made available to citizens. Information needed by civic activists or organizations to maintain oversight and challenge local officials on their management of public facilities may be withheld, even when the information's relevance to any possible terrorist threat is at best tenuous.

In the same document, the CJOG recommended that federal agencies should preserve public access to what it calls *critical oversight information*—"any information a citizen might use to judge whether his or her public servants are serving well," information "that speaks to the quality and integrity of their performance as policy makers, managers or employees of our seaports, airports and transit systems," including budget information and details on revenue and spending and information about personnel and their qualifications, training, and performance.

22.5 Controls on Environmental Impact Information

Controls on environmental impact information are premised on the need to protect internal agency decision-making procedures and to control access to information that terrorists might use to harm critical infrastructures, deliver services, or poison the air, water, and so forth. The actions discussed next represent steps that have been taken to safeguard public access to environmental information.

22.5.1 Categorical Exclusions to FOIA

The DHS expanded its ability to withhold certain types of environmental impact information that previously was available to the

public pursuant to the National Environmental Policy Act (NEPA). On June 14, 2004, DHS issued a directive proposing new categorical exclusions to disclosure requirements under FOIA for assessments of environmental impacts of DHS decision making and included component DHS agencies in the categorical exclusions policy. The directive specified three levels for projects or grants that might have environmental impacts: "those affecting national security that are categorically excluded from coverage under NEPA; those that require DHS agencies to conduct environmental assessments; and those with the greatest potential to affect natural resources and the environment, which would require more detailed environmental impact statements." Specifically, NEPA allows categorical exclusions for "actions that … do not … have significant impact on the human environment, and therefore … do not require an environmental assessment … or environmental impact statement…." (40 C.F.R. 1500–1508). Some of the agencies that were transferred to DHS had previously identified such exclusions.

22.5.2 Exemptions

The directive also exempted all DHS agencies (TSA, Coast Guard, Border Patrol, Federal Emergency Management Agency, and others) from releasing classified, proprietary, or other information exempt from disclosure under FOIA, and proposed to exempt CII, SSI, and other information described in "laws, regulations, or Executive Orders prohibiting or limiting the release of information." Some say this could exclude from public view environmental impact statements required by NEPA. In its Federal Register announcement, DHS said that it would place protected information prepared for compliance with NEPA into appendix sections for viewing only by decision makers, but would allow the public to view nonsensitive portions of the material. However, it added that "… if segregation would leave essentially meaningless material, the DHS elements will withhold the entire NEPA analysis from the public." The plan would also allow DHS to categorize some environmental reviews as SSI or CII exempt from public disclosure. The public comment period was for 1 month and then was extended to August 16, 2004. DHS held a meeting on October 12, 2004, to discuss public comments received. No further

publicly announced information appears to have been released about this policy.

A 2005 supplemental appropriations bill (H.R. 1268), enacted as P.L. 109-13, exempted the DHS from certain legal requirements when physically securing U.S. borders. Some contend that this may enable DHS to waive environmental protection laws, among others, relating to border security.

22.5.3 Critiques of Controls on Environmental Information

Some critics allege that these types of policies, including SBU information control policies, conflict with the environmental quality laws of the 1970s and the Emergency Planning and Community Right-to-Know Act of 1986 (42 U.S.C. 11049). Critics of regulations limiting access to some CII focus on their preemption of state and local disclosure laws and the inability of citizens to obtain information needed to ensure community safety. Several environmental groups have criticized controls on environmental information, including the DHS environmental directive released on June 14, 2004.

The Natural Resources Defense Council charged that because the agencies subsumed by DHS make environmentally related decisions relating to oil spills, border security, flood planning, and chemical plant security, and so forth, communities should be given an opportunity to evaluate these decisions. Some agencies also label environmental impact statements as SBU, saying that they should be released only to those who have a need to know. Some agencies post environmental impact materials on the Internet with blacked-out markings for what appears to be location or infrastructure detail.

Other agencies have published documents and put SBU information into a separate appendix, available under controlled access. Generally, because of security sensitivity, most DOE environmental assessment documents are not available to the public online but may be accessible via hardcopy in NEPA reading rooms if the requestor qualifies.

The American Library Association proposed that, with respect to environmental information, DHS should limit "its non-disclosure provision to information that unambiguously qualifies for with-holding under one of the exemptions provided in the Freedom of Information

Act…." It contended that the provision allowing DHS to withhold essentially meaningless information not now subject to exemption from disclosure should be deleted because Congress intended the public to determine what information is meaningful in the environmental statements. OMB Watch concurred: "There are no procedures contained in the directive for how DHS will determine which pieces of environmental analysis to remove if it falls within an exemption, or how it will determine if the public finds the information meaningful."

22.5.4 The Nuclear Regulatory Commission (NRC) Example

The complexity of balancing access to, and protection of, information is illustrated by actions taken by the NRC. In August 2004, the agency issued a statement that "certain security information formerly included in the Reactor Oversight Process will no longer be publicly available." Its efforts to scrub its website while balancing public access and information security generated public criticism that NRC withheld information relevant to the safety of surrounding residents but shared such information with power companies and industrial lobbying groups. The NRC also allegedly threatened criminal prosecution for persons who published critiques of two nuclear reactors in Indian Point, New York, even though the NRC is reported to have said it could not specify what information was compromised. In fall 2004, some "… news and watchdog organizations pointed out that some sensitive documents in the (NRC online) library could be used by terrorists." The NRC subsequently closed major portions of the library and reviewed items it contained.

Representative Edward J. Markey, a senior minority member of the House Committee on Energy and Commerce, wrote to the NRC, requesting that its inspector general investigate the agency's information release policies and, specifically, concerns about the NRC "improperly restricting access to specific documents that should be releasable from a security perspective but are nevertheless being withheld from public release." He cited the agency's proposals to widen its definition of *proprietary information* to withhold more public information and to broaden restrictions on the dissemination of sensitive information to include emergency evacuation plans and safety analyses concerning the protection of nuclear materials; its actions to

withhold an unclassified version of a National Academy of Sciences (NAS) report allegedly because the NRC disagreed with its findings; and the agencies' prohibitions on nonindustry representatives attending meetings and having information, even though industrial representatives were given access. In June 2005, the NRC announced it would restore viewing on the web to more than 70,000 documents, after reviewing them for SSI.

An NRC task force concluded that the agency could withhold information that could be deemed useful to terrorists if the information were not already available to the public pursuant to its new Sensitive Information Screening Project, but FOIA principles needed to be followed to withhold information. The task force identified the precise kinds of information that could be withheld under the various FOIA exemptions. Also during this period, the National Academies released an unclassified version of a report that included among its findings that the commission's security restrictions on the sharing of information with industry and the public negatively affected "constructive feedback and cooperation. The committee recommended that the … NRC improve the sharing of pertinent information on its security analyses of spent fuel storage with nuclear power plants operators and system vendors. More constructive interaction with the public and with independent analysts also could increase confidence in … NRC and industry decisions and their actions to reduce the vulnerability of spent fuel storage to terrorist attacks."

22.6 Controls on Unclassified Biological Research Information

22.6.1 Dual-Use Concerns

Traditionally, open communication of biological information fosters the conduct of research and development. Also, emergency preparedness requires exchange of information to inform local health officials "… of what agents are being studied in their jurisdictions so they can prepare for any unlikely future events." However, some biological information and data could pose a domestic or international security threat, which has led to federal controls. For instance, a 2006 National Academies report described a variety of biotechnology agents and specific genetic advances that could be used in research and could increase the potential for biowarfare. It also inventoried

some dual-use biological agents and research developments that could be used malevolently. For example, "the same reverse genetic technologies that can be used to develop new vaccines against RNA viruses could also be used to construct modified viruses, including possibly viruses that express heterogonous virulence factors that result in more lethal disease."

Ominously, it observed that

> [in] the past, dual-use concerns have focused on pathogens and on the challenges associated with controlling dangerous pathogens. As already emphasized, this committee's deliberations have indicated that the problem will be far broader and more profound in the future. For example, advances in neurobiology may make it possible to manipulate behavior and thought processes, while gene expression technologies just now coming to fruition will make it possible to activate endogenous molecules in the body—with possibly wide ranging and everlasting effects. Advances in synthetic biology and nanotechnology will offer similar rich opportunities for dual use. Nano-devices that may be used to unplug blocked arteries could instead be employed to interfere with circulatory function.

22.6.2 Governmental Control Proposals

"Advanced drug delivery technologies and pharmacogenetics knowledge could be used to develop and deliver with greater efficiency new bio-weapons, perhaps even selectively targeting certain racial or ethnic groups." To deal with concerns like these, some types of biological sciences information have already been controlled and proposals have been made to develop other types of governmental or nongovernmental systems to control access to information before research is conducted or in the prepublication phase. These proposals, which are discussed next, are not without controversy.

The federal government's regulation requiring the registration of laboratories that transferred certain select agents—organisms and toxins identified by the Centers for Disease Control and Prevention (CDC) as potentially useful in bioterrorist activities—began in 1996. Registration of laboratories that possess such agents was mandated by P.L. 107-188, The Public Health Security and Bioterrorism

Preparedness and Response Act of 2002, enacted after the 9/11 attacks. The law requires coordination between the Department of Health and Human Services (DHHS) and the Department of Agriculture to identify and regulate the use and transfer of such agents that pose a risk to public health, crops, or livestock; registration of all facilities that use such agents; minimum safety requirements for registered facilities; background screening of persons using such agents; and a national database of such users. The USA PATRIOT Act, P.L. 107-56, prohibits access to select agents by certain persons, including certain immigrants and persons with criminal or drug use history and other factors. Interim final regulations implementing these laws were issued in December 2002.

22.6.3 National Science Advisory Board for Biosecurity

A NAS report, *Biotechnology Research in an Age of Terrorism: Confronting the "Dual Use" Dilemma*, published in 2004 and dubbed the *Fink* report after the committee chairman, called for greater self-regulation by scientists, use of institutional biosafety committees at academic and research institutions to monitor research that could possibly aid terrorism, National Institutes of Health (NIH) review of certain types of research reports before they are published, and use of screening criteria in a prepublication review. Regarding private scientific publishing, the Fink report largely left it up to journal publishers to make decisions about prepublication review procedures for articles involving biological agents. The Fink report also urged the creation of a new federal advisory board to guide nongovernmental researchers and to develop responsibility among scientists to control flows of biodefense information.

But it did not propose governmental control of such research. In March 2004, the DHHS announced its intent to create a National Science Advisory Board for Biosecurity (NSABB), which became funded in 2005. It is managed and staffed by the NIH. The NSABB is chartered to have 25 voting nongovernmental members with a broad range of expertise in molecular biology, microbiology, infectious diseases, biosafety, public health, veterinary medicine, plant health, national security, biodefense, law enforcement, scientific publishing, and related fields. The NSABB also includes nonvoting

ex officio members from 15 federal agencies and departments. It is supposed to advise federal departments and agencies regarding oversight of dual-use nonclassified biological research. The board's charter also includes work to develop national policies to communicate and publish sensitive research results, a code of conduct for life sciences researchers, training programs and materials to educate the community about biosecurity, and strategies to foster international collaboration to oversee dual-use life sciences research. NIH aims to use the committee's guidance to develop policies to require performer institutions that it funds to use Institutional Biosafety Committees (IBC), to educate researchers, to issue guidance, and to review and advise on specific experiments that might be misused or pose a threat to the public health or national security. Policy guidance will flow from the federal board to the institutional committees if there is uncertainty or disagreement regarding denial of an experiment. The NSABB met in June 2005 and November 2005, and also in 2006.

During its first meeting, the board established five working groups to develop criteria to identify dual-use research; criteria to communicate results of dual-use research; a life sciences code of conduct; international perspectives on dual-use research; and guidance on chemical synthesis of bacterial and viral genomes. Some discussants proposed that biologists should be licensed to conduct sensitive biological research, that codes of conduct would need to be certified, and that methods of assuring compliance among research institutions would need to be developed. Some contended that if the scientific community did not develop methods of monitoring and protecting sensitive research, policy makers might develop and try to enforce more stringent controls that ultimately might prove to be unacceptable. During the November 2005 meeting, the working groups gave progress reports and discussed developing guidelines, including the use of risk-based procedures.

22.6.4 Views on Adequacy of Biosecurity Protection Policies

22.6.4.1 2006 National Academies Report Some critics say existing biosecurity protections are inadequate to prevent terrorists from obtaining and using biological information and suggest that stronger measures should be taken, such as creation of a network that interacts

closely with intelligence and military agencies to prevent misuse of biological information. Related to this, a 2006 National Academies report, concerned about how new developments in the life sciences coupled with rapidly advancing fields such as nanotechnology and materials science could prove to be threatening, endorsed the free and open change of information in the life sciences to the maximum extent possible. However, it also recommended the following:

- "… Creating statutorily an independent advisory group in the security community to strengthen scientific and technical expertise within the intelligence and security communities
- Adopting and promoting a "common culture of awareness and a shared sense of responsibility within the global communities of life scientists," including development of codes of ethics
- Establishing "… a decentralized, globally distributed network of informed concerned scientists who have the capacity to recognize when knowledge or technology is being used inappropriately or with the intent to cause harm" and whose interventions could take the form of counseling or "… reporting such activity to national authorities when its appears potentially malevolent in intent"

22.6.4.2 Inadequate Rules Other shortcomings in current policy have been identified. For instance, the scope of the DHHS's NSABB board has been faulted because it does not extend to privately funded research nor harmonize international standards. Others criticize the select agent rules as inadequate and say federal regulations should be expanded to prevent unauthorized persons from possessing the DNA components of a select agent. George Church, a genetics professor at Harvard, reportedly "is organizing a consortium of researchers and academics to push the federal government to license anyone interested in purchasing DNA segments for agents of bioterror." Similarly, John Steinbruner and colleagues at the Center for International and Security Studies at Maryland, in a 2005 report, advocated mandatory licensure of researchers and institutions that conduct biodefense research. Three levels of independent review—at the institutional, national, and international levels—would monitor risks and benefits

of research proposals and would issue approval or disapproval for conduct of researchers and publications.

22.6.4.3 Codes of Conduct/Self-Monitoring Policies Nongovernmental professional groups have explored the use of codes of conduct or self-monitoring policies for research topics and publications. Some publishers adopted a set of voluntary, risk-based publishing principles, called *Statement of Scientific Publication and Security*," in 2003; but this, reportedly, has resulted in changes in only very few articles before publication. In June 2005, the American Society for Microbiology drafted a code of ethics for its members and urged them to report to appropriate authorities misuses of microbiology information. The Interacademy Panel on International Issues, consisting of most of the world's national science academies, issued a set of principles that urged scientists to take responsibility to prevent misuse of their work. Two researchers, Margaret A. Somerville of McGill University and Ronald M. Atlas, president of the American Society for Microbiology, proposed an international code of ethics to prevent bioterrorism. Adherents to the code would refuse to conduct work that could be used in bioterrorism and would seek to restrict access of those they believe could use information maliciously.

22.6.4.4 Peer Review It was noted above in the section on "Nongovernmental Experts' Recommendations to Use Risk Analysis to Identify and Control Sensitive Information" that proposals have been made to instill in researchers a culture that discourages research that could be used malevolently, that professional peer reviews should be conducted before publication of work that should be protected, and that the federal government should define policy controls for these activities. J. Gaudioso and R. M. Salerno also proposed a biosecurity risk assessment process that would restrict the use of agents that have the potential to be weaponized and that could serve as the basis for international standards. This process would involve using four biosecurity levels: low, moderate, high, and extreme risk. The overwhelming majority of pathogens and toxins would fall into the low-risk category (requiring practices such as locking unattended laboratories and maintenance of documentation of agents used), and most select agents would be placed in the moderate-risk category

(requiring additional safeguards such as access controls and personnel checks).

22.6.4.5 Risk Categories The security measures for low- and moderate-risk categories should pose reasonable costs and largely rely on existing biosafety measures. Few agents would be designated high risk (requiring more stringent security measures and a dedicated biosecurity officer). Perhaps only *Variola major* (the most severe form of smallpox), because it is no longer found in nature, would be considered an extreme risk, requiring the most stringent protections (such as comprehensive background investigations and an on-site guard force). Higher security than that currently mandated by federal regulations would be applied only for those very few agents that represent true weapon threats. Biosecurity levels should be developed and vetted by experts in biological weapons, microbiology, security, and public and agricultural health. This would help federal agencies apply uniform criteria to grantees and could form the basis for standardizing biosecurity internationally.

22.6.4.6 Risk-Based Approach Brian J. Gorman proposed a risk-based alternative approach for prepublication peer review. He called for a risk-based process called *Due Process Vetting System* (DPVS) together with "… a Risk Assessment Scale (RAS) and a Least Restrictive Classification System for the communication, assessment, and disposition of sensitive life science research in a manner consistent with national security interests." The process would be overseen by a new agency called the Biologic Regulatory Commission (BRC), modeled after the NRC. The vetting process would be triggered at the request of an author or peer reviewer if an article attained a predetermined score on the RAS set by the BRC. "The RAS surveys opinions of informed reviewers including the author of the article, the author's Institutional Review Board or Institutional Biosafety Committee (IBC), and finally the journal interested in publishing the article." The DPVS would safeguard high-risk articles by providing the government with a mechanism to identify "potentially dangerous articles before they reach the presses," would avoid the "deleterious effects of censorship," and would make articles available only to a "select academy of biodefense researchers after the

authors, the publishing journal and others, reach a consensus with the government through cooperative vetting of the article in question." Gorman proposed expanding the academy to a qualified body of world scientists, an approach he said is superior to the American Society of Microbiology (ASM) model and ad hoc approaches undertaken by the majority of U.S. biosciences journals.

22.6.4.7 Restrictions Frustrate Researchers Some scientists disagree with the types of aforementioned restrictions. Existing controls on select agents, reportedly, have caused "… many researchers … to discontinue or not pursue research on regulated biological agents, rather than implement the new security regulations and bear the associated financial burden. Reportedly, the CDC expected 817 entities to register under the new select agent rule. Instead, only 323 facilities are registered with the CDC, which indicated that many institutions have discontinued their work with select agents." There are also complaints that U.S. select agent rules can hinder cooperation from foreign scientists who cannot afford security controls and that many foreign laboratories do not meet the standards for conducting such research demanded by the U.S. government. As a result, foreign partners, some charge, may be forced to become mere sample exporters, and criminal sanctions might be applied to the U.S. partner in a foreign collaboration if the foreigner partner's laboratory does not meet U.S. research security standards. Complaints about the CDC's information security manual have led to concern by influenza researchers that the CDC is not releasing databases of virus sequences and other data needed to develop flu vaccines, thereby potentially damaging the development of public health protections.

22.6.4.8 Ethics Education Option At the first NSABB meeting, some members also suggested that instead of formal restrictions, ethics education for researchers would suffice to deal with potential problems. Others suggest that controls on biological research information could constrain the exchange of information needed to develop effective defenses against dangerous pathogens. A National Academies report, *Seeking Security; Pathogens, Open Access and Genomic Data Bases*, published in 2004, that had been requested by

the National Science Foundation and the CIA, concluded that there should be no change in current policies that allow scientists and the public unrestricted access to genome data on microbial pathogens. Access, it concluded, improves the nation's ability to fight both bioterrorism and naturally occurring infectious diseases. Open access to raw sequence data is unlikely to help bioterrorists develop weapons—and preventing distribution of such information could hurt research to prevent bioterrorism and emerging diseases such as Severe Acute Respiratory Syndrome (SARS). Genomic information about most dangerous pathogens is already available, it said, and if the government wants to restrict distribution of information in the future, such information should be classified. The report concluded that security against bioterrorism would be achieved best by policies that facilitate, not limit, the free flow of this information. In May 2005, the DHHS attempted to prevent the NAS from publishing an article in the *Proceedings of the National Academy of Sciences* on how the U.S. milk supply could be tainted with botulism and control measures to prevent it. The academy published it on the grounds that the benefits of publishing the paper giving biodefense guidance outweighed any threats.

22.6.4.9 UK Royal Society/Welcome Trust 2004 Paper Other nations and international scientific groups have addressed this issue. For instance, reportedly, a December 13, 2004, paper issued jointly by the United Kingdom's Royal Society and the Welcome Trust urged caution on government intervention. The joint paper said that "government should ask scientific societies and funding institutions to take more responsibility for vetting and preventing the dissemination of risky technical details. The paper suggested that grant review forms could include a check box for bioterror issues to ensure that they are considered." Also, at a meeting in June 2005 in Geneva, life scientists from several countries sought to develop a code of conduct. Biosafety in life sciences research was also a topic of discussion at an Organization for Economic Cooperation and Development International futures program meeting in September 2004, and the National Academies held an International Forum on Biosecurity in Como in March 2005 to discuss convergence on codes of conduct and oversight of biosecurity research.

22.7 Issues Dealing with Geospatial Information

There is considerable controversy about providing access to certain types of geospatial information, including satellite imagery and maps depicting ordinary facilities, and so forth.

22.7.1 RAND Corporation's Three Filters

Supporting more open access to such information, in March 2004, the RAND Corporation released a study recommending that the federal government should not remove geospatial information such as maps and imagery from public availability because much of it is not current enough to meet terrorists' needs, terrorists can obtain such information from other sources, and the public benefits from access to much federal geospatial information. Instead, it recommended that the federal government develop an analytical process to assess the potential homeland security sensitivity of specific publicly available geospatial information using three filters: usefulness, uniqueness, and societal benefits and costs.

22.7.2 Homeland Security Guidelines

Subsequently, in June 2005, the Homeland Security Group of the Federal Geographic Data Committee, an 18-member federal interagency group that coordinates geospatial data, issued for consideration interim and then final guidelines for public, private, and nonprofit organizations that originate and publicly disseminate geospatial data. The guidelines seek to balance "security risks and the benefits of geospatial data dissemination" and suggest how organizations can use risk-based procedures to provide access to data while protecting sensitive information. The group observed that safeguarding is justified only for data that contain sensitive information that is difficult to observe and not available from open sources, that are the unique source of the sensitive information, and for which the security risk outweighs the societal benefit of dissemination. Two options were offered to handle sensitive data before public release—changing it to remove or modify the sensitive information by summarizing it, blurring details, and so forth; or restricting the data but maintaining it in

original form and making it available to those who need it, such as first responders.

22.7.3 FOIA Exemption

Congressional action in 2004 tightened controls on some geospatial information. Section 914 of P.L. 108-375, the Defense Authorization Act FY2005, signed on October 28, 2004, authorized a new FOIA exemption 3 category permitting the withholding from public disclosure of land remote sensing information prohibited from sale to non-government or government-approved customers for reasons of national security and under license as described by the Land Remote Sensing Policy Act of 1992 (15 U.S.C. Section 5601 et seq.). Such information may not be exempted from disclosure to Congress; information disclosed to state or local government may not be made available to the public; and agencies are required to protect such information from disclosure.

22.7.4 National Geospatial Intelligence Agency (NGIA) Example

On November 18, 2004, the DOD's NGA announced that for security reasons, as well as for reasons of potential intellectual property rights violations for information gathered commercially in other countries, it would "… remove its Flight Information Publications (FLIP), Digital Aeronautical Flight Information File (DAFIF), and related aeronautical safety of navigation digital and hardcopy publications from public sale and distribution." After the review of comments was completed in November 2005, the agency implemented its plan. However, its rationale for removal of information focused exclusively on the intellectual property rights issue, not the security dimensions.

22.7.5 Expanding Use of Data

In contrast to restraining information, legislation has been introduced to expand use and applications of federal remote sensing data. During the 109th Congress, H.R. 426, Remote Sensing Applications Act of 2005, reported favorably on June 27, 2005 (House Report 109-157), would, among other things, direct the Administrator of the National

Aeronautics and Space Administration to establish a program of grants for pilot projects to explore the integrated use of sources of remote sensing and other geospatial information to address state, local, regional, and tribal agency needs. It requires the administrator, when awarding grants, to give preference to specified types of projects. The bill did not contain language constraining use of data.

22.8 The DHS's SBU Directives

22.8.1 Controversy and Opposition

The DHS issued an internal management directive (MD 11042) on "Safeguarding Sensitive but Unclassified (For Official Use Only) Information" on May 11, 2004, to safeguard SBU information within DHS. Such information would be labeled For FOUO and would be defined "to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest." Portions of the memorandum generated considerable opposition because of its mandatory and punitive employee and contractor nondisclosure requirements. In January 2005, the controversial requirements were replaced with requirements to educate employees in security practices, and the document was reissued as MD 11042.1. Contractors are still required to sign nondisclosure agreements, and DHS employees and contractors are still subject to administrative or disciplinary action for violating the policies.

22.8.2 Types of Control Labels

The directive identified several types of control labels that could be SBU, including FOUO, CII, and SSI and so forth and 11 types of sensitive unclassified information that can be designated FOUO—a type of SBU—by any DHS employee, consultant, or contractor. The list includes one clearly identifiable technology-related item, which conceivably might include the results of DHS-sponsored or conducted scientific research and development:

(k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

22.8.3 Unclassified and Need to Know

P.L. 107-296 specified that, if practicable, DHS's research is to be unclassified, but the presidential signing statement may have mitigated this provision. It remains to be seen how this SBU regulation will affect information generated by DHS-funded research and development grants and contracts, and what the response will be of universities that conduct research for DHS under its academic centers of excellence programs.

Access to the information covered by the DHS SBU directive is on a need-to-know basis, and information can be shared with cleared homeland security personnel at state and local levels. The directive said the use of the FOUO designation did not automatically exempt information from disclosure under FOIA but "information requested by the public under a FOIA request must still be reviewed on a case-by-case basis." The information would retain the FOUO designation until the originator or other officials determine otherwise. Procedures to protect and disseminate such information outside of DHS were spelled out, including requirements for secure storage and suggestions for encrypted Internet and telephone communications. Some other agencies also require employees to sign nondisclosure agreements in order to protect SBU information.

22.8.4 Complete CRS Report

For the complete text of CRS report for Congress "*Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information*, visit the Federation of American Scientists' website at http://www.fas.org/sgp/crs/secrecy/RL33303.pdf.

23

Operation Security

A Law Enforcement Concern

23.1 The Role of Operational Security

Many law enforcement agencies take a blasé attitude toward operational security. However, in the current environment of sophisticated criminals and potential terrorist activities, the role of operational security should be reviewed.

It is crucial that law enforcement operational methods and sources remain confidential. Reality television has been a positive learning experience for the public, but also a negative influence as it serves as a school for criminals and terrorists. To learn how law enforcement agencies plan, collect intelligence, conduct raids, respond to high-risk calls, and generally operate, all one has to do is watch television. Even more disturbing is that the methods used by forensic scientists in gathering trace evidence have also been openly presented.

23.2 Information Sources for Criminals

What are some of the sources from which criminals/terrorists can gather data about your agency?

23.2.1 Press Releases/Media Stories

Press releases and media stories present a common source. Agencies love to brag on their operations or accomplishments, and in doing so, may release critical data as to methods of operations, available

resources, intelligence-gathering techniques, and names of agency individuals involved.

23.2.2 Agency Websites

Agencies usually have extensive information on their websites (including special response teams such as SWAT, bomb squad, and precision marksmen). Carefully review what is presented and use caution in responding to requests for information about the agency. One agency proudly shows its special response team in full equipment on its website. This gives an adversary a very good idea of the number of personnel available, type of body armor worn, firearms used, etc. Photographs of personnel, other than command grade personnel, should be avoided, as this may compromise undercover operations if the officers are recognized.

23.2.3 E-Mails and Online Chat Rooms

E-mail may not be secure. If it is not encrypted, then you must assume it is subject to being intercepted. Keeping sensitive material in a nonsecure area such as a residence or on a home personal computer is not recommended. Additionally, do not leave such materials in a vehicle. The use of chat groups online can be another source of release of sensitive information. You never know who is in the chat room.

23.2.4 Surveillance of Communications

Other methods commonly used to gather information include surveillance of communications. Agencies that use nonencrypted radios for communications can be intercepted and should not be used to discuss sensitive information. Cellular telephones, although convenient, are another source of information because the calls can be intercepted.

23.2.5 Surveillance of Activities

The surveillance of activities is yet another way criminals can gather data. Some adversaries are smart enough to use various indicators to identify law enforcement capabilities, plans, and operations. Vice

officers were astounded while on a raid in one southern city to find photographs of unmarked and covert police vehicles and a list of license plate numbers belonging to police officers personal vehicles. The drug traffickers were intelligent enough to conduct counter surveillance and identify officers. They read and watch the media, use open sources such as websites, obtain building plans from open sources, and are very observant. These groups use indicators such as the type vehicle, antennas, and radios located inside vehicles to identify unmarked police cars. An adversary may observe the comings and goings of personnel to the agency to identify normal operations with variances indicating a special operation is in progress. Monitoring of radio traffic for unusual volume or use of encrypted radios may be another indicator of police activities. Pizza services laughingly state they know when the military is conducting special operations when they get large orders of pizza from the Pentagon after normal business hours.

23.2.6 Trash Receptacles

Trash is a fertile source of intelligence. Many agencies discard important documents in the trash. In some agencies, this trash is handled by inmates who have access to some of the most sensitive documents the agency produces. Trash should be shredded with a professional shredder that cross cuts the paper into unreadable shreds or chips. Mundane items such as purchase orders or telephone call slips can provide an adversary vital information.

23.2.7 Sensitive Documents

Document security is another facet of operational security that when jeopardized can lend information to enemies. Plans and vital data should be marked as *Confidential* or *Law Enforcement Sensitive*. They should not be stored on a computer server outside control of the agency. One agency used brightly colored paper for all law enforcement sensitive material, making it easier for personnel to identify it. However, it was found to be counterproductive. The items were being protected while in the offices, but were routinely being discarded in the trash without being shredded. Inmate laborers had recovery of sensitive material made easy by the brightly colored documents.

A special effort should be made to clearly mark all law enforcement sensitive documents, and they should be secured. Rosters that contain the names of personnel, their home addresses, telephone numbers, etc., are especially sensitive and should be closely guarded.

23.3 Preventing Breach of Security

Tips to help prevent this invasion of privacy and breach of security are listed below.

23.3.1 Countersurveillance

Countersurveillance should be conducted by all law enforcement personnel.

23.3.2 Do Not Discuss Sensitive Information

Do not discuss sensitive law enforcement information with family members and/or non–law enforcement friends. They may unintentionally release information that might be critical to an operation.

23.3.3 Secure Firearms and Weapons

Security of weapons is an important issue particularly for law enforcement specialty teams. It is very embarrassing and a great civil liability when a firearm is accessed by unauthorized personnel. One agency had to deal with a negative media fallout when a SWAT member left an automatic carbine on the top of his vehicle and drove away. The weapon was later found and stolen by a passerby. Fortunately, the weapon was recovered and the suspect arrested before its use. Another agency had to deal with the loss of several pounds of explosives by a bomb detection canine handler. The explosives were eventually recovered. If personnel are losing critical items such as firearms and explosives, what does this say about the potential for theft? One specialty team member had an explosive grenade that dispensed rubber buckshot and tear gas stolen from a storage shed at his residence. Weapons and munitions should always be securely stored in a locked location that is theft resistant.

23.3.4 Monitor Inmate Labor

Inmate labor is common in law enforcement and must be closely monitored. In many regards, it may be the only janitorial services available to an agency. Steps must be taken to restrict the prisoner's access to sensitive materials and areas. Imagine the chagrin one agency faced when an inmate assigned to janitorial duties was able to retrieve a stolen credit card from an investigator's desk. The inmate also obtained the keys to an unmarked police vehicle and fled the state using the stolen credit card. Another agency routinely used inmate labor to clean firearms after officers' range qualifying. Remember these are criminals and should be closely supervised while operating in and around a public safety facility.

23.3.5 Restrict Information Sharing with Other Agencies

Always use extreme caution with disclosing any law enforcement sensitive material. Other agencies, such as emergency management, fire, and emergency management system (EMS), routinely operate with law enforcement. Most of their employees are trustworthy; however, one item to remember is that the background investigations and job requirements are not as stringent. Therefore, it is not uncommon to find persons with criminal records, or even convicted felons, working for these agencies. One law enforcement agency discovered a firefighter was being considered for an EMS role on their special response team, but he was also a member of a right-wing extremist group.

23.3.6 Vigilant Background Checks for Clerical and Information Technology (IT) Personnel

Always perform careful background checks. Clerical and IT personnel in many agencies have broader access to sensitive materials than does the average line officer. Vigilant background checks are needed to ensure that they are not security risks. Some outlaw biker gangs specifically target law enforcement by attempting to insert a person into a clerical position. A disgruntled or dishonest employee also presents a threat to the agency. This should be remembered in allowing access to sensitive materials.

23.3.7 Personal Security

Remember your personal security. Unlisted telephone numbers, using banking institutions for loans and credit, and limiting personal information on surveys are just a few ways to limit the spread of personal information. Avoid having your own web page, and do not post photographs of yourself or family members on any website. Have your law enforcement magazines sent to your agency address if permissible.

23.4 Developing a Security Plan

Every agency should take countermeasures that include a comprehensive operational security plan. The plan must address how documents are handled and the methods to ensure that sensitive information does not end up in the trash. Secure communications should be provided for along with precepts for limiting sensitive information to only those who need to know. Specialty team commanders and team members should consider methods to reduce indicators of their operations. A holistic and comprehensive plan scaled to the individual agency needs with proactive steps to assure security is a necessity.

24

Camera Surveillance

DENNIS TREECE

Director of Security, Massachusetts Port Authority

24.1 Setting up Camera Surveillance

Many companies and agencies find that setting up electronic camera surveillance improves security in especially sensitive areas. For instance, a business that uses a mainframe for its database may want to set up an electronic camera that can record who accesses the mainframe. If data are stolen, the camera record may help identify who was responsible.

In this section, you will find useful information on designing a camera surveillance program for your company or agency.

24.1.1 Step One: Decide on Purpose

Determine what you want your cameras to do for the company. This will help you decide just about everything else regarding the system. There are two main uses for camera surveillance: prevention and image capture for later uses.

24.1.1.1 Prevention Prevention means real-time detection and monitoring so actions can be taken immediately. This is labor force intensive and extremely expensive to pull off.

24.1.1.2 Capturing Images for Later Use Capturing images for later use in determining what happened and who/what was involved is a more realistic approach in most cases, but each situation is different and each company needs to decide for itself which approach is most appropriate.

24.1.1.3 Combination Approach A combination approach is always possible, with detection and prevention in the high-crime areas and forensic use for all other cameras. In one organization, personnel decided that the camera surveillance system was primarily for forensic use, so that after any incident of interest (accident, crime, terrorism, over-crowding, etc.) they would be able to review the images and back everyone up from the event to the edge of the property to see who they talked to, what car they drove, where they parked, what bus or taxi they got out of, and what condition the facility was in at the time (icy sidewalk, wet floor, tools in the area, etc.). The organization also determined that it would not be able to watch the cameras all the time, but when called by someone with an incident report, it could call up the camera with best coverage and monitor the situation. Finally, the organization did decide that certain areas were so important that smart cameras should do constant watching, and send an alarm when something began to happen.

24.1.2 Step Two: Assess Existing Technology

If you have cameras already, you need to conduct a survey as to what departments own them, what they are for, how they are monitored, and what format they use, and then decide if any of these cameras can be folded into your new system.

24.1.3 Step Three: Decide Details

Become more informed on camera surveillance technologies and their impact on operations, training, maintenance, and staffing levels. Determine how clear you need the picture to be (as opposed to how clear you want them to be), as this will have a significant impact on cost to build the system and run it. Here are some of your choices.

24.1.3.1 Frame Rate The more frames per second you choose, the more network capacity each camera will require and the more data storage you will need. A famous Fortune 50 company uses 3 frames per second (fps) to watch cash registers and their studies showed that no human could trick the camera in a third of a second. Another company uses 10 fps because the analytical software requires a minimum

of 7 fps and it can only use multiples of 5 fps. The closest above 7 fps is 10 fps. Note here that if you are expecting to catch a baseball in flight you will want a high frame rate, possibly 30 fps or full motion video—but again, that is going to be very expensive to operate.

24.1.3.2 Resolution The clearer your picture, the more pixels it will have, the larger the file it will require, and the more bandwidth it will consume. This is exactly the same issue as with frame rate, but it is not a motion issue, rather it is a clarity issue. Studies determined that 1/4 common intermediate format (CIF) (1/4 as clear as your TV at home) is perfectly OK to provide an image to the police that they can use to find and apprehend a suspect. If you expect to get mug-shot quality out of your video surveillance program then you will want full CIF, but you will pay for it in terms of bandwidth and storage.

24.1.3.3 Compression There are several standard commercial compression algorithms available, but the most common, for all the right reasons, is MPEG-4. Many have chosen this format because it is economical in its functionality and it has high clarity and ease of use needed. You can add a commercial compression package to your MPEG-4 to further reduce your storage needs.

24.1.3.4 Storage Duration Thirty days of storage is pretty much the unofficial national standard for data storage. This typically gives enough time to learn of an incident before the data are lost, without overdoing it. When you get an event of interest, you should plan on dropping that file to a DVD to store it indefinitely—or at least until all criminal and civil proceedings are concluded, as well as any appeals. You can also send events of interest to a separate server for indefinite storage.

24.1.3.5 Storage Size A single digital camera running 24 hours at just 5 fps, using MPEG-4, at 1 CIF resolution creates 11 gigabytes (GB) of information. That is 330 GB in 30 days for just one camera! A 500-camera system, not at all uncommon for corporate buildings and campuses, will generate 165 terabytes (TB) every month. It is easy to see why keeping images past 30 days, when there is nothing special in them, is economically foolhardy. And remember, this is with

cameras running on spare settings as noted above. Full motion video (30 fps) will create 990 TB of data, or almost a petabyte. If you also go to full CIF, just multiply by 4! So be very careful to stay on top of the original engineering discussions with your contractors and consultants, because they can easily overdo your system with very large cost consequences. Remember to keep them on track with what you want the cameras to do. Mission creep in those discussions can be expensive. And remember, it is not just storage, but also bandwidth you have to consider. How are you going to move 5500 GB of digital video through your network every month?

24.1.3.6 Digital versus Analog At some point, you will want to convert your images to digital in order to take advantage of the much easier storage, as well as the retrieval and search capabilities it gives you. Remember, analog images travel farther from the camera so cable runs will impact your choices. Get a good consultant who you trust to advise you on the best route to go.

24.1.3.7 Pan Tilt Zoom (PTZ) There are two ways to do this. The old fashioned way, which still works really well, is to physically move the camera and change its focus to get a close-up view of an event. Dome cameras, which have a dark bubble over the camera, help to mask where the camera is pointed at any given time. Make sure each PTZ has a default park position that gives you an optimal view and focal length. It is easy for these cameras to be left where it was last focused, which will likely not give you the best coverage when nothing special is going on. The other way to do PTZ is digitally, within the image itself. This will require megapixel images because zooming in on, say, a license plate, will fuzz out, beyond the ability to read it, if you do not start with sufficient pixel density in your camera platform. Obviously, digital PTZ is a lot more expensive than physical PTZ.

24.2 Issues to Consider

24.2.1 Monitoring

This is a very contentious issue. While the public may expect that surveillance cameras are monitored all the time, it is just not practical

or even possible. The best you can do is put your high-priority camera images up in your command center for occasional viewing. If you have analytics, that is, software that can pinpoint an event of interest and call it up with an audible alarm, then you have the best of both worlds—constant monitoring without having to watch until something happens that needs some sort of response.

24.2.2 Decoys

While you may be tempted to use dummy camera domes to make people think you have surveillance, it will also give your public a false sense of security. Most competent programs avoid the use of dummy cameras except in very unique circumstances and then only when in conjunction with live cameras.

24.2.3 Staffing

It is normally unrealistic to expect additional staff to monitor a new suite of cameras, and it is equally unrealistic to expect different staff than the people you have now. For these reasons, you will want to choose a system that has a simple graphical user interface, provides out-of-service alarms for cameras and encoders, is low-maintenance, and has high mean times between failures.

24.2.4 Privacy

Make absolutely certain you supervise the troops who have access to the camera images and who have access to the PTZ cameras. If you do not, it is inevitable that your cameras will be diverted to personal, voyeuristic use that can obviously have a seriously negative impact on your company image, internally and externally, once that is publicized—and it will be.

24.2.5 Signage

Get advice from your legal counsel regarding the use of signs that announce the use of video surveillance on your property.

24.2.6 Policies and Procedures

If your cameras can view geography off your property, consult with your software provider to mask out these areas. This is especially important if you have line of sight to residential properties. Supervision and the application of swift discipline are very important to avoid the inappropriate use of your cameras.

24.2.7 Training

The more complex your system, the more training the staff will need. This takes good time management because unless you have a full shift to go on training rotation, you will be doing training on overtime.

24.2.8 Maintenance

Be sure to include in your maintenance contract a service level agreement that guarantees that your high-priority cameras are fixed promptly. Be sure it includes an adequate stock of on-site replacement cameras and network encoders and other peripheral devices so when things go down they can be restored to service quickly. Your system should open a trouble ticket as soon as there is a device failure, and you will want to review the system's performance monthly to ensure you have current knowledge on how reliable it is and which parts are providing the most difficult.

25

Eavesdropping Threats and IP Phone Systems

25.1 Eavesdropping Threats

25.1.1 Influences on Eavesdropping

Protecting one's information against the threat of technical interception, or eavesdropping, is complicated by the variety of techniques that the eavesdropper has at his or her disposal. If he or she is determined to intercept the information, he or she may employ any or all combinations of techniques. The level of his determination will be influenced by the value of the information (to the perpetrator).

The problems presented by the area in which the eavesdropper must operate will also influence the choice of techniques. Those items that will limit the techniques at his or her disposal include the physical standards and safeguards in the target area, personal capabilities, and access to specialists who can broaden his/her capabilities.

*25.1.2 Evaluating the Threat**

In evaluating the technical interception threat, several questions must be answered:

1. What is the value of the information to the potential eavesdropper?
   A: This value, which may be completely different from its value to the owner of the information, tends to establish the threat level (the extent and expense to which the eavesdropper will go to gain the information). It also

* The information provided in this section was retrieved from TSCI Technical Security Consultants, Inc. (http://www.dbugman.com).

establishes, to some extent, the risk the eavesdropper will take to acquire the information. Obviously, if the information is of relatively low value, the eavesdropper will expend relatively little time and money and expose himself to very little risk.

2. Who constitutes the threat?
   A: This question is best answered by determining who can benefit from the interception. Depending on who and what benefit can be determined, there is some basis for an analysis of technical capability and the probability that a specialist will be employed.
3. What is the desired duration of the interception?
   A: If the duration is short (a 2-hour conference, for example), some interception techniques are more convenient and likely to be used than others. If the desired duration is an extended one (such as continuous monitoring of an office), techniques requiring batteries in the target area are much less likely to be used.
4. What other operational constraints are imposed on the eavesdropper?
   A: In answering this question, one must realize that the eavesdropper requires three successful links to accomplish his purpose:
   - He must have a concealable means of conveying the physical energy of the conversation to a medium that can be transmitted;
   - He must have a concealable means of transmitting (wire, light beam, radio, etc.); and
   - He must have a location and the terminating equipment necessary to transform the transmitted data back to a form that can be used. Both the location and equipment must be concealed.

   If any one of these three links are detected or prevented, the eavesdropper has failed.

25.2 IP Phone Systems

Rainer A. Melucci, CSC, CFC, DABFE, CHS-III P.I.

25.2.1 Explanation of IP

Over the past few years, the technology associated with voice communication has changed dramatically. Although these advancements have vastly broadened our abilities as far as resource sharing and feature deployment, they have also created the possibility of higher-level breaches in security. The system currently deployed is known as an IP Phone System. The term *IP* is an acronym for Internet Protocol.

An IP Phone System works as a network of phones or nodes whose data are managed by a series of routers and switches. These systems are often referred to as Voice over IP (VoIP) networks. The structure of these networks is generally very similar to the structure of the data network instituted for your computer systems. Many times, the phone system and computer system are in such a topology that they can share resources and be integrated.

25.2.2 Threats Associated with IP Systems

Most people today are aware of the security threats associated with computers, but it is important to remember that a phone system based on the same principles falls victim to the same problems.

25.2.2.1 Remote Access A prime issue for concern is the ability to access the system remotely from outside the premises. Some technology experts might say that the remote access feature should simply be disabled; however, by doing that a vast number of important features become unusable.

25.2.2.2 Packet Sniffing Another major concern is packet sniffing. Any system that is IP-based or transmits data over a data bus uses packets as its method of transportation. If those packets are being intercepted and then analyzed, any conversation or information would be compromised. It would be impossible to create a list of every possible breach.

25.2.3 Security Measures

In order to properly assess a system such as this, these measures should be put into place:

- An independent technology firm should be contracted to review the topology of the routers and switches associated with the system.
- Next, a certified systems engineer for the product line should be contacted to check the general structure.
- Once both of those professionals concur on a rough draft of the system's design, an in-depth analysis of the programming, system permissions, and access rights should be made.
- It would also be in your best interest to handle the situation as a double blind; one contractor should know of your true intentions for investigation, while the other should be unaware.

25.2.4 NIST Recommendations

The NIST offers these recommendations for setting up and providing for the security of a VoIP network. The section that follows is an excerpt from a 2005 NIST special publication entitled *Security Considerations for Voice over IP Systems*. Note that point 1 is highly technical and will probably be understood only by IT professionals.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.
    - Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate dynamic host configuration protocol servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection.

- At the voice gateway, which interfaces with the public switched telephone network, disallow H.323, session initiated protocol (SIP), or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients toward a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or Transport Level Security [TLS] to protect SIP signaling.)
- Use IP security (IPsec) or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP private box exchange access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems

(including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

An especially challenging security environment is created when new technologies are deployed. Risks often are not fully understood, administrators are not yet experienced with the new technology, and security controls and policies must be updated. Therefore, agencies should carefully consider such issues as their level of knowledge and training in the technology, the maturity and quality of their security practices, controls, policies, and architectures, and their understanding of the associated security risks. These issues should be considered for all systems but are especially important with VoIP deployment for essential operations, such as systems designated high under FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

VoIP can provide more flexible service at lower cost, but there are significant trade-offs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack. Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained.

An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VOIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully

planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

   Unlike traditional telephone connections, which are tied to a physical location, VOIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the trade-off is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

   Unless the VoIP network is encrypted, anyone with physical access to the office local area network (LAN) could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies, therefore, should ensure that adequate physical security is in place to restrict access to VoIP network components.

   Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking, this means that installation

of a sniffer could result in not just data but all voice communications being intercepted.

5. Evaluate costs for additional power backup systems that may be required to ensure continued operation during power outages.

   A careful assessment must be conducted to ensure that sufficient backup power is available for the office VoIP switch, as well as each desktop instrument. Costs may include electrical power to maintain uninterruptible power supply (UPS) battery charge, periodic maintenance costs for backup power generation systems, and cost of UPS battery replacement. If emergency/backup power is required for more than a few hours, electrical generators will be required. Costs for these include fuel, fuel storage facilities, and cost of fuel disposal at end of storage life.

6. VoIP-ready firewalls and other appropriate protection mechanisms should be used. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

   Because of the inherent vulnerabilities (e.g., susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

7. If practical, softphone systems, which implement VoIP using an ordinary personal computer with a headset and special software, should not be used where security or privacy is a concern.

   Worms, viruses, and other malicious software are extraordinarily common in personal computers connected to the Internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised website. Malicious software attached to e-mail messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These

vulnerabilities result in unacceptably high risks in the use of softphones, for most applications. In addition, because personal computers are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

8. If mobile units are to be integrated with the VoIP system, use products implementing Wi-Fi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

   The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WPA, a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the FIPS 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher-level cryptographic protocols and applications such as SSH, TLS, or IPsec with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

9. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

   Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors.

26
Facility Security

Much of the information presented in this chapter was retrieved from the American Council for Technology and Industry Advisory Council. It applies mainly to federal agencies, but the issue dealt with is of interest to any organization wanting to improve security using such technology as smart cards.

26.1 Homeland Security Presidential Directive 12

In the wake of the September 11 attacks, President Bush released HSPD-12, or Homeland Security Presidential Directive 12, entitled Policy for a Common Identification Standard for Federal Employees and Contractors. He issued the directive on August 27, 2004.

In the first section, President Bush states: "Wide variations in the quality and security of forms of identification used to gain access to secure federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees)."

To assist in the creation of HSPD-12 identification cards, the NIST wrote FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, detailing the credentialing processes, technologies for the cards, and the ways they will be managed. FIPS 201 standardizes the approach to meeting the homeland-security objectives behind HSPD-12. The standard covers verifying a person's identity (known as identity proofing in the industry), registering to obtain a card, issuing the card, revocation, and maintaining records. The PIV standard consists of two parts—PIV-I and PIV-II. PIV-I

satisfies the control objectives and meets the procedural security and privacy requirements of HSPD-12, while PIV-II meets the technical interoperability and technological security requirements of HSPD-12.

26.2 Who Manages the PIV Program?

Several groups must cooperate to implement PIV-I and PIV-II, under strong management leadership. Human resources, the physical security department, and the office of the chief information officer (CIO) are likely candidates. The privacy officer must be involved. All must work together in a cooperative manner.

Note: In your agency or company, only one organization or individual should have overall responsibility for leading and managing your HSPD-12 program, recognizing its importance as a foundation for shared identity information in both logical and physical access control systems, even where these systems are managed independently.

Smart cards and technology are only pieces of HSPD-12, and have already been well proven in many implementations. Implementing a PIV-compliant process will likely present more challenges than deploying the appropriate technology. Effective organizational and change-management leadership will be critical in ensuring a smooth transition across the agency or organization. For example, it may seem obvious, but it is essential to decide who will be given cards. Not so obviously, you must determine the information that will be gathered about these individuals. Will they need different levels of access? Will they need access to varied IT applications?

Because a variety of personal data may be needed, some agencies have left HSPD-12 responsibility to human resources.

Other agencies already have authentication-credential issuance tightly coupled to physical access.

Yet other agencies have strong logical-authentication regimes or may have implemented authentication technologies based on industry-supported standards such as Security Assertion Markup Language or specifications from industry organizations such as Liberty Alliance. For these agencies, the CIO organization may be the appropriate place for leading the HSPD-12 program.

Remember that whatever leadership option is selected, all stakeholders must be closely involved in planning and implementation so that their specific needs are addressed.

New capabilities must be created and all impacted organizations must work together. Policies and procedures must be created, adapted, refined, and harmonized.

Agencies with strong interagency interaction at a business or functional level must implement HSPD-12 in a manner that ensures that interagency access and sharing mechanisms are effectively coordinated and interoperable.

The next sections of this road map provide key requirements and issues that need to be addressed by agencies as they consider their implementation of HSPD-12.

26.3 What Do You Need to Implement PIV-I?

Do you know what your HSPD-12 obligations and timelines are? Note that although the implementation date for PIV-I has passed, it is not clear to what extent all agencies have met all requirements. Given the importance of PIV-I, it is necessary to highlight key PIV-I obligations and issues:

- Have you submitted a PIV-I plan to the Office of Management and Budget (OMB)? (See OMB Guidance M-05-24.)
- Do you have an identity proofing and registration process? (Federal Identity Management Handbook, Attachment A, Section 2.2, and Appendix B)

Note: With NIST FIPS 201 and special publications, agencies should not rely solely on the Federal Identity Management Handbook. However, it is a valuable compendium of information and information sources.

- Will your current method of screening applicants and issuing the credentials satisfy the requirements of HSPD-12?
- Do you have established locations where employees apply for badges and receive them?
- Will the methods serve as locations for your long-term HSPD-12 needs? (FIPS 201-1)

- Are your current application and issuance processes documented? Will your current method of screening applicants and issuing the credentials satisfy the requirements of HSPD-12?
- Are the roles and responsibilities of personnel who issue credentials compatible with the roles defined in HSPD-12? (FIPS 201-1, Appendix A, Section A.1; and the Federal Identity Management Handbook, Attachment A, Section 2.2; and Appendix B)
- Do you have a process for instituting security checks, updating records with updates from inquiry results, and securely storing information for new employees, old employees, and contractors? (FIPS 201-1 Section 2.2) If yes, are they national agency check with inquiries (NACI) or an OPM equivalent? (FIPS 201-1 Section 2.2)

Note: As the OMB implementation plan addresses both PIV-I and PIV-II, agencies will need to determine if a PIV credential can be issued prior to completion of the NACI or if a temporary card should be used.

- Do you have HSPD-12 language in new contracts? If no, discuss with your contracting officer. (OMB Guidance M-05-24)
- Does your process address registering citizens of foreign countries? (FIPS 201-1 Section 2.2)
- Is your process certified and accredited in accordance with NIST Special Publication 800-79?
- Have you complied with all 10 privacy requirements, including such measures as assigning a senior agency official for privacy, conducting comprehensive privacy impact assessments, and maintaining an appeals procedure for those who are denied credentials or whose credentials are revoked?

Note: As suggested above, remain aware of any new guidance from OMB on factors for successful implementation.

If you can confidently answer yes to all of these questions, you probably have fulfilled your PIV-I obligations. Your next step is to prepare to implement PIV-II.

26.4 What Do You Need to Prepare for PIV-II?

An HSPD-12 system will not exist in a vacuum. Along with establishing clear lines of authority and responsibility as well as a program office to manage agency transition, you must closely monitor information and guidance from OMB and NIST. The following questions will help you assess where you are and where you need to go, and they will narrow the path to get there.

26.5 Integration with Existing Infrastructure

Your HSPD-12 solution must operate within your existing infrastructure. Integration of PIV cards into legacy physical and logical access control systems is a challenge that must be addressed in the initial planning. Some elements include the following:

- Do you have badging systems?
- Do you have a current and accurate functional assessment of your badges and all badging systems in use?
- Do you have an inventory of all components?

Note: The old badging system may not be able to maintain the chain of trust mandated by HSPD-12. However, certain components such as existing data records, computers, cameras, or scanners may be reusable in an HSPD-12 solution, thus saving considerable implementation costs.

- Have you assessed your physical access control systems (for example, building entrance systems, gates) to determine what features are needed on your PIV card to support these systems (for example, bar code, magnetic strip, RFID, biometrics)?
- Do you have an understanding of what current ID cards are used for and when they will need to operate in parallel until applications and systems are migrated to the new credential (e.g., current tokens may be used for photocopier access or similar purposes)?
- Have you assessed your logical access control systems (for example, for access to computer systems, applications) to determine whether you need additional network capability or

additional fields on your PIV card chip to support these systems (for example, additional public key infrastructure [PKI] certificates, biometrics, passwords)?
- Do you have a migration strategy for moving to the new system?
- Have you budgeted for the cost of migration?
- Are you using a PKI?
- Is your PKI cross certified with the Federal Bridge Certification Authority?
- If not, you must choose to use a shared service provider (SSP) to purchase your certificates. (Federal Identity Credentialing Committee Shared Service Providers [SSP] Subcommittee Certified Providers List)
- Do you have an electronic connection to OPM to conduct clearance requests and background checks?
- Is your interface automated?
- Can your existing interface be used for the HSPD-12 solution? (FIPS 201-1)

Note: Many agencies go directly to the FBI and may need to determine how to link the fingerprint check from the FBI with the OPM name check, and whether a manual or automated process is most practicable.

- Do you have an automated system for storing and retrieving personnel data and files?
- If yes, will it meet HSPD-12 requirements? (FIPS 201-1)

Note: Agencies may find that existing components, if they are put together, will not meet HSPD-12 requirements because they will not be capable of supporting a chain of trust.

The issues addressed above are fundamental for effectively implementing PIV-I and PIV-II to support HSPD-12. However, they are not comprehensive. Secure hosting, certified card issuers, and other issues must also be addressed. Agencies must also deal with defining and implementing an issuance system, smart cards, and evaluating options for leveraging this new authentication infrastructure to improve access control, current and future applications, and strategic, government-wide initiatives.

Finally, agencies should review PIV-I policies and decisions to be sure that they in fact migrate to PIV-II, and manage new approaches evolving since the PIV-I deadline, such as the consideration of a national shared enrollment system where a single facility is shared by multiple agencies within a given area.

PART VII
Identity Theft

CHAPTER 27 Fair and Accurate Credit Transactions Act
CHAPTER 28 Identity Theft Red Flags under FACTA
CHAPTER 29 Development and Implementation of a Red Flags Prevention Program

27

Fair and Accurate Credit Transactions Act

27.1 Overview

Identity thieves use an individual's personal identifiable information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. Financial institutions and creditors will be required to implement a program to identify, detect, respond, prevent, and mitigate identity theft risks known as *red flags*. Identity theft is a growing concern that ultimately erodes the fabric of one of our most consumable critical infrastructures under homeland security—our financial industry. Many security departments, fraud departments, or corporate investigative departments will be required to develop and implement an identity theft red flags program, or at a minimum, assist with assessing the identity theft risk to their organizations. This course will provide you with an overview of assessing, developing, and implementing a red flags program.

27.2 What Is FACTA?

The Fair and Accurate Credit Transactions Act of 2003 is also known as FACTA or FACT Act. FACTA was enacted in 2003 and amends the Fair Credit Reporting Act (FCRA), a federal law that regulates, in part, who is permitted to access your consumer report information and how it can be used. Section 114 and Section 315 of FACTA are related to Identity Theft Prevention and Address Discrepancies for identity theft red flags. FACTA requires each financial institution or creditor to develop and implement a written identity theft prevention program.

27.2.1 Section 114 (Special Rules for Card Issuers)

Section 114 of FACTA, also known as Special Rules for Card Issuers, requires

- The agencies to jointly issue guidelines for financial institutions and creditors regarding identity theft; and
- Establishing reasonable procedures that assist creditors and financial institutions in identifying identity theft and set forth provisions specifically applicable to debit and credit card issuers who receive notice of a customer's change of address.

27.2.2 Section 315 (Address Discrepancy Rules)

Section 315 of the FACTA amends Section 605 of the FCRA, 15 United States Code, 1681c, requires

- Providing a notice of the existence of a discrepancy if the address provided by the customer/accountholder in its request substantially differs from the address of the consumer reporting agency in its consumer file for the customer accountholder;
- Procedures to handle a notice of address discrepancy; and
- Users of credit reports to establish reasonable procedures for handling a notice of a significant discrepancy between a credit report and application for credit.

27.3 What Agencies Promulgated the Red Flags Rule?

There were six federal agencies involved in promulgating identity theft red flags rules:

- Department of Treasury—Office of the Comptroller of the Currency under 12 Code of Federal Regulation (CFR) Part 41
- Federal Reserve System under 12 CFR Part 222
- Federal Deposit Insurance Corporation under 12 CFR Parts 334 and 364
- Department of the Treasury—Office of Thrift Supervision under 12 CFR Part 717

- National Credit Union Administration under 12 CFR Part 717
- Federal Trade Commission under 16 CFR 681

27.4 FACTA Guidance

The red flag rule applies to financial institutions and creditors with covered accounts with no regard whether credit reports are obtained.

Appendix J to Part 571 provides interagency guidelines on identity theft detection, prevention, and mitigation. Appendix J of the red flags rule lists examples of possible patterns, practices, and forms of activities creditors should consider when implementing a written identity theft prevention program.

27.4.1 Financial Institutions

Financial institutions are defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a transaction account belonging to a consumer. Most of these institutions are regulated by federal bank regulatory agencies or National Credit Union Administration (NCUA). This definition also includes financial institutions under the Federal Trade Commission's (FTC) jurisdiction, which includes chartered credit unions and certain other entities that hold consumer transaction accounts.

27.4.2 Creditors

A creditor is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. For example, creditors include finance companies, financial institutions, automobile dealers, mortgage brokers, hospitals, mortgage bankers, non-banking financial services companies, utility companies, and telecommunication companies, to name a few. Most creditors, except for those regulated by federal banking

regulatory agencies and NCUA, fall under the jurisdiction of the FTC. It is estimated that FACTA identity theft red flags rule may potentially impact 11 billion businesses.

27.4.3 Covered Accounts

Covered accounts are accounts used mostly for personal, family, or household purposes that involve multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft—for example, small business or sole proprietorship accounts.

Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

27.4.4 Transaction Accounts

Transaction accounts are deposit or other accounts from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

27.5 Penalties for Non-Compliance to Red Flags

27.5.1 Federal

Federal enforcement by the FTC Act, Title V, may bring an enforcement action up to $2500 in penalties for each violation of the red flag rule.

27.5.2 State

State enforcement by the state attorney general's office may recover up to $1000 for each violation plus attorneys' fees.

27.5.3 Civil

Civil lawsuits by consumers may be entitled to recover actual damages sustained from a violation of the red flag rule, plus attorney fees.

27.6 Benefits of Complying to Red Flags

- Customer trust for protecting their personal identifiable information
- Reduction in risk for negative publicity
- Reduction in risk to covered accounts
- Reduction in risk of lawsuit
- Reduction in risk to operational fraud
- Reduction in risk to identity theft

28

Identity Theft Red Flags under FACTA

28.1 Red Flags

28.1.1 Definition

A red flag is defined as a pattern, practice, or specific activity that indicates the possible existence of identity theft. The red flags rule is designed to protect consumers or covered accounts from the most common types of identity fraud. While the following examples are a starting point for the identification of red flags, they are not intended to be an all-inclusive list or checklist of what organizations can experience or classify as a red flag.

28.1.2 Examples of Red Flags

FACTA has 26 examples of red flag activities or elements within Supplement A to Appendix J in five categories:

1. Alerts, notifications, or warnings from a consumer reporting agency
   a. A fraud or active duty alert is included with a consumer report.
   b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
   c. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
   d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as

i. A recent and significant increase in the volume of inquiries
ii. An unusual number of recently established credit relationships
iii. A material change in the use of credit, especially with respect to recently established credit relationships
iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor

2. Suspicious documents
   a. Documents provided for identification appear to have been altered or forged.
   b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
   c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
   d. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
   e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
3. Suspicious personal identifying information
   a. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor, such as
      i. The address does not match any address in the consumer report
      ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File
   b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there

is a lack of correlation between the SSN range and date of birth.

c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example,
   i. The address on an application is the same as the address provided on a fraudulent application
   ii. The phone number on an application is the same as the number provided on a fraudulent application
d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor, such as
   i. The address on an application is fictitious, a mail drop, or a prison
   ii. The phone number is invalid, or is associated with a pager or answering service
e. The social security number provided is the same as that submitted by other persons opening an account or other customers.
f. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
g. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
h. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
i. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. Unusual use of or suspicious activity related to the covered account
   a. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
   b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns, such as
      i. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry)
      ii. The customer fails to make the first payment or makes an initial payment but no subsequent payments
   c. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example,
      i. Nonpayment when there is no history of late or missed payments
      ii. A material increase in the use of available credit
      iii. A material change in purchasing or spending patterns
      iv. A material change in electronic fund transfer patterns in connection with a deposit account
      v. A material change in telephone call patterns in connection with a cellular phone account
   d. A covered account that has been inactive for a reasonably lengthy period is used (taking into consideration the type of account, the expected pattern of usage, and other relevant factors).
   e. Mail sent to the customer is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the customer's covered account.
   f. The financial institution or creditor is notified that the customer is not receiving paper account statements.
   d. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding identity theft
   a. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that has opened a fraudulent account for a person engaged in identity theft.

28.2 Identity Theft Defined

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another individual's personal identifiable information or data in some way that involves fraud or deception. There are four common types of identity theft: financial, social security, medical, and criminal/character. Identity theft is an international crime and is not just about credit (Figure 28.1). An identity theft red flags prevention program is a mitigation strategy to reduce risks in this area.

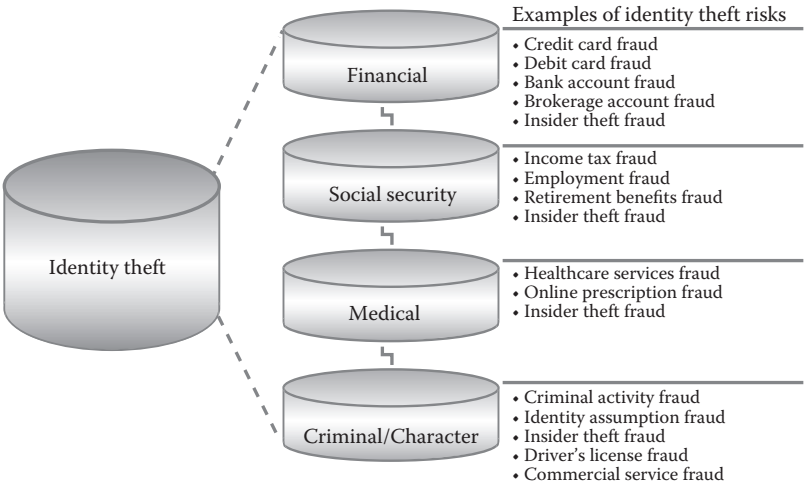

Figure 28.1 Types of identity theft.

28.3 Types of Identity Theft

28.3.1 Four Main Risk Areas

Organizations should identify, quantify, and consider four main risk areas when assessing the extent of identity theft. Based on the extent and the combination of the given risk areas, the overall risk to a customer or customer data can increase as various risks elements are introduced.

28.3.2 Personal Identifiable Information (PII)

PII is data or data points, a name, or number that may be used, alone or in conjunction with any other information to identify a specific person, including

- Name
- Social Security number
- Date of birth
- State or government ID card
- State or government driver's license
- Alien registration number
- Passport number
- Employer ID number
- Taxpayer ID number
- Fingerprint or voice print
- Retina or iris image
- Other physical representations
- Electronic Identification Number
- Street address
- E-mail address
- Routing Code
- Credit or debit card with PIN
- Telecommunication identification or access device

29

Development and Implementation of a Red Flags Prevention Program

There are two core areas of developing and implementing a FACTA identity theft red flags program—establishing a written program and administering the program.

29.1 Written Program

Establishing a written program, which includes a risk assessment and charter, is one of the core areas FACTA identity theft red flag program identifies as necessary. Each identity theft red flags prevention program should have a detailed written program designed to address the governance, implementation, and maintenance of the program through policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or the safety and soundness of the financial institution or protect creditors from identity theft. As part of the written program, a charter or mission statement document should be developed and approved by the organization's board of directors. If the organization is a small- or medium-sized business, the business owner or the senior manager of the organization should approve the charter or mission statement.

29.1.1 Charter

A charter or mission statement document is customarily two to four pages and includes, but is not limited to, the following items:

- Introduction
- Statement of management commitment

- Purpose of the charter
- Scope of the charter
- Executive signoff page

29.1.2 Risk Assessment

29.1.2.1 Identify Overseer Once the charter is developed, it is essential for the organization to identify a Chief Identity Theft Officer (CITO), Chief Compliance Officer (CCO), identity theft champion, or a senior level manager to oversee the development, implementation, and administration of the identity theft red flags prevention program. Many organizations form a cross-functional working committee with an identity theft champion or senior level manager as the team lead. Once the champion is chosen and a cross-functional team is selected, it is incumbent to begin conducting a risk assessment and devising the administration to the program.

29.1.2.2 Collect Information The CITO or CCO will need to research and obtain a variety of internal and external documents to complete the identity theft red flags risk assessment to include, but not limited to, the following (Figure 29.1):

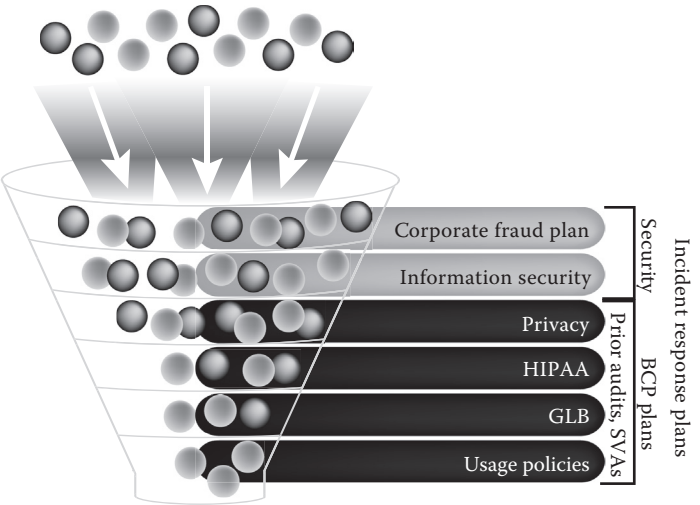

Figure 29.1 Identity theft risk assessment documentation.

- Business Continuity and Incident Response Plans Prior audits, inspections, policies, or security vulnerability assessments (SVAs)
  - Gramm–Leach–Bliley Safeguard Procedures
  - HIPAA Security Rule Procedures
  - Current Data/Information Security Procedures/Policies
  - Responsible Use Policies
  - Code of Conduct/Ethics Policies
  - Customer Identification Program Policies/Procedures
- Prior audits, inspections, policies, or SVAs
  - Bank Secrecy Act Procedures
  - Privacy Policy/Procedures
  - Know Your Customer Procedures/Policies
  - Current Corporate Anti-fraud Plans
  - Current Corporate Investigation/Security Plans
  - Any third-party data security or fraud assessments within the last 24 months

29.1.2.3 Establish a Risk Assessment Team Once the necessary documents have been collected and reviewed, the CITO or CCO will need to conduct an identity theft red flags risk assessment. Before the identity theft red flags risk assessment, the CITO or CCO should develop and establish an identity theft red flags risk assessment team. The identity theft red flags risk assessment team should comprise team members with different skill sets and functional knowledge in corporate security, corporate fraud, corporate investigations, new account set-up, anti-money laundering, customer service, account servicing, information security, legal, privacy, and information technology.

29.1.2.4 Identify Risk Assessment Methodology The CITO and the assessment team will need to adopt or identify a risk assessment methodology for conducting the identity theft red flags risk assessment. In general, the identity theft red flags risk assessment methodology might be a risk-based, performance-based, or any type of quantitative process to measure risk (Figure 29.2).

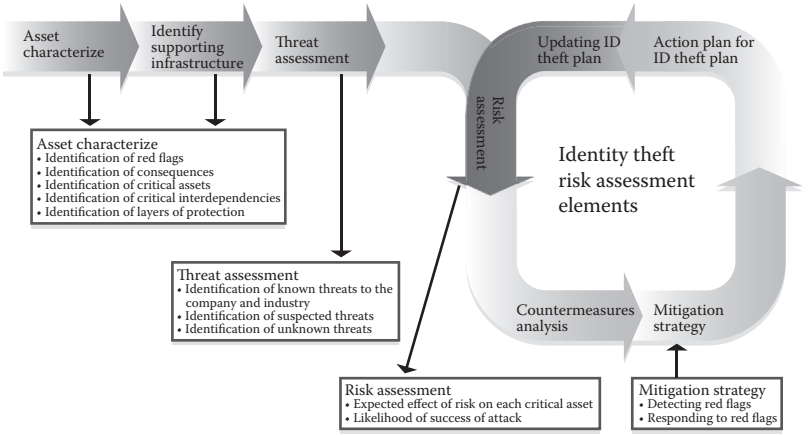

Figure 29.2 Identity theft risk assessment elements.

29.1.2.5 Conduct the Risk Assessment Now, the CITO, CCO, or senior manager has conducted research and leveraged internal/external documents, established an identity theft red flags assessment team, and developed an identity theft risk assessment methodology. The assessment is performed by conducting an on-site survey or assessment using the following strategies:

- Review and evaluate policies/procedures for alerts, notifications, or warnings from a consumer reporting agency for existing covered accounts and new accounts to include addresses, other customer account information, and associated risks.
- Review and evaluate policies/procedures for setting up new accounts and servicing existing accounts.
- Review and evaluate policies/procedures for suspicious documents for covered accounts.
- Review and evaluate policies/procedures for suspicious personal identifiable information for covered accounts.
- Review and evaluate policies/procedures for unusual use of or suspicious activities related to covered accounts.
- Review and evaluate policies/procedures for notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding identity theft in connection with a covered account.

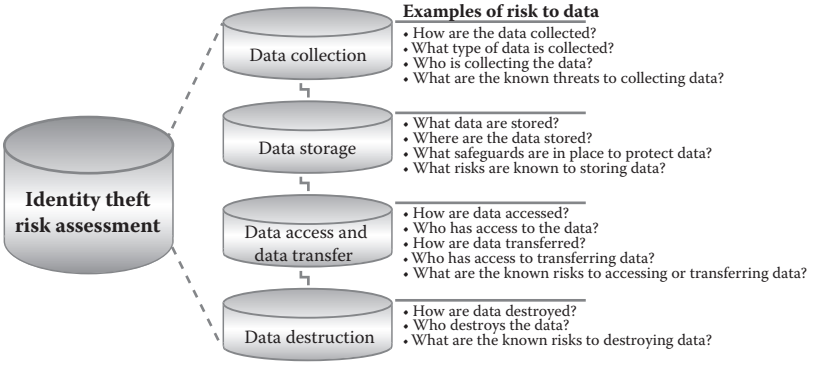

Figure 29.3 Risk assessment process.

- Review and evaluate incident response policies/procedures for covered accounts.
- Review and evaluate privacy and information usage policies/procedures for covered accounts.
- Review and evaluate service provider, vendor, third-party and subcontractor agreements, or service level agreements in an effort to revise or implement reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft to any covered accounts or covered account information accessed, stored, transferred, or destroyed by service providers, vendors, third parties, or subcontractors.
- Review and evaluate information technology/information security policies/procedures for collecting, accessing, storing, transferring, and destroying information.

29.1.2.6 Identify Theft Risk to Data Organizations should also consider the data risks when assessing and evaluating the extent of identity theft to covered accounts or covered account information (Figure 29.3).

29.2 Administering the Program

The program administration should include reasonable policies and procedures for detecting, identifying, preventing, responding, and mitigating identity theft risks and relevant patterns, practices, and forms of red flags signaling possible identity theft associated with the

organization's business environment. The program administration should also include written verbiage regarding employee, contractor, and vendor awareness training for identity theft, protection of personal identifiable information, and data security. The training should identify frequency, methods, requirements, and maintaining training records for employees, contractors, and vendors.

29.2.1 Identifying Relevant Red Flags

A critical element of developing and implementing an identity theft red flags program is identifying relevant red flags for covered accounts. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to

- Identify red flags for covered accounts offer by the organization
- Identify the methods used to open new accounts and associated red flag risks
- Identify the methods used to access covered accounts and associated red flag risks
- Identify red flags for existing accounts
- Identify the methods used to service existing accounts and associated red flag risks
- Identify the methods used to access existing accounts and associated red flag risks
- Identify any previous experiences with identity theft related to covered accounts
- Identify any current or previous experience with identity theft related to your specific industry

29.2.2 Detecting Red Flags

A crucial element of developing and implementing an identity theft red flags program is detecting red flags for covered accounts. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address the detection of red flags in connection with the opening of covered accounts and servicing existing accounts, such as

- Detecting red flags for covered accounts offered by the organization
- Detecting red flags by authenticating or monitoring covered accounts or activities for evidence of identity theft
- Obtaining identifying information about and verifying the identity of a person opening a covered or existing account

29.2.3 Responding to Red Flags

An essential element of developing and implementing an identity theft red flags program is responding red flags for covered accounts. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address responding to red flags in connection with the opening of covered accounts and servicing existing accounts, such as

- Responding appropriately to any red flags that are detected to prevent and mitigate identity theft.

29.2.4 Preventing and Mitigating Identity Theft

A critical element of developing and implementing an identity theft red flags program is preventing and mitigating identity risks. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address the risk of identity theft posed to the customer or account, such as

- Monitoring an account for evidence of identity theft
- Contacting the customer to validate activity or information
- Changing any passwords, security codes, or other access to a customer's account
- Re-opening an account with a new account number
- Not opening a new account
- Closing an existing account
- Notifying law enforcement
- Determining that no response is warranted

29.2.5 Updating the Program

A vital element of developing and implementing an identity theft red flags program is updating the identity theft red flags program. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address updating the program, such as

- Updating the program periodically to reflect new developments and changes in the risk environment relating to identity theft
- Annually reporting to the board of directors or senior management on the program effectiveness, service provider arrangements, significant identity theft incidents, and recommendations for program changes

29.2.6 Establishing an Identity Theft Training Program

An essential element of developing and implementing an identity theft red flags program is establishing an identity theft training program. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address identity theft training for implementing the program and continuous training for employees, contractors, or vendors with responsibilities for opening, servicing, or accessing covered accounts, such as

- Identifying relevant red flags for covered accounts
- Detecting red flags for covered accounts
- Responding appropriately to any detected red flags
- Incident response preparedness, contingency, recovery, and continuity planning for red flags events
- Identity theft awareness for covered accounts
- Social engineering scenarios for identity theft red flags
- Handling customer accounts or personal identifying information

- Identity theft red flags assessments and inspections
- Knowledge of current identity theft threats and patterns
- Assessment of identity theft red flags tests, drills, and exercises
- Review of the Identity Theft Prevention Program

29.2.7 Oversight of Service Provider Arrangements

A vital element of developing and implementing an identity theft red flags program is ensuring oversight of service providers, vendors, third parties, and subcontractors who collect, access, store, transfer, or destroy covered account information. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to ensure oversight of third parties, such as

- Service providers, vendors, third parties, and subcontractors complying by implementing reasonable policies and procedures designed to identify, detect, respond, prevent, and mitigate the risk of identity theft to covered accounts or covered account information
- Assigning of specific responsibilities for program implementation
- Reviewing reports by staff and approving of material changes in the program
- Reporting at least annually on compliance with the program
- Facilitating the written program approval from the board of directors

29.2.8 Obtaining Approval of the Initial Written Program by the Board of Directors

A vital element of developing and implementing an identity theft red flags program is ensuring buy-in and approval of the written program by the board of directors. In order to ensure the identity theft red flags program is taken seriously and fully implemented, the written program must be approved by the organization's board of directors or an appropriate board committee.

29.2.9 Address Discrepancy Rules

The address discrepancy rules offer several examples of reasonable policies and procedures that the user (i.e., financial institution or creditor) of a consumer report can adopt as such.

29.2.9.1 Comparing Information Users can compare the information in the consumer report provided by the consumer reporting agency. With information, the user can

- Obtain and use it to verify the consumer's identity in accordance with the requirements of the customer identification program (CIP)
- Maintain its own records, such as applications, change of address notifications, or retained CIP source documents
- Obtain information from a third-party source
- Verify the information in the consumer report provided by the consumer reporting agency with the consumer

29.2.9.2 Develop Reasonable Policies and Procedures The address discrepancy rules also require the user of consumer reports to develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from which it received the notice of address discrepancy. The user (i.e., financial institution or creditor) of the report needs to

- Be able to form a reasonable belief the consumer report relates to the consumer about whom the user requested the report
- Have established a continuing relationship with the consumer
- Regularly and in the ordinary course of business furnish information to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer, from which the notice of address discrepancy relating to the consumer was obtained

29.2.9.3 Confirm the Address The user (i.e., financial institution or creditor) may reasonably confirm the address is accurate by

- Verifying the address with the consumer about whom it has requested the report
- Reviewing its own records to verify the address of the consumer
- Verifying the address through third-party sources
- Using other reasonable means

29.2.10 Special Rules for Card Issuers

A crucial element of developing and implementing an identity theft red flags program is special rules for card issuers. The program strategy must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address the validity of change of address notifications.

29.3 Maintaining an Identity Theft Red Flags Program

After establishing a program, it is essential to maintain the program maintenance for the identity theft red flags program. The program must be tailored to the size and complexity, and the nature and scope of the financial institution or creditor operations, and must contain reasonable policies and procedures to address maintaining the effectiveness and compliance of the program, such as

- Developing and maintaining a documented strategy for identity theft metrics
- Devising and documenting a self-assessment strategy and methodology for evaluating the identity theft red flags program
- Providing an annual identity theft awareness training for all employees and contractors
- Providing continuous identity theft awareness to employees with identity theft responsibilities
- Developing and devising a documented strategy and procedure for auditing the identity theft red flags program
- Developing and devising a documented outreach strategy for customer care in the area of identity theft prevention and notification

- Developing and devising a documented strategy and procedure for continuous monitoring of covered accounts to identify or reduce risks associated with identity theft
- Developing and devising a documented strategy and procedure to test, drill, and exercise the effectiveness of the identity theft red flags program
- Developing and devising a documented strategy and procedure for periodically determining whether covered accounts pose a foreseeable risk of identity theft
- Developing and devising a documented strategy and procedure for tracking, trending, and conducting a pattern analysis on identity theft-related events or incidents

Bibliography

Customer Identification Programs, 68 C.F.R. 103.121.
Department of the Treasury—Office of the Comptroller of the Currency—12 Code of Federal Regulation (C.F.R.) Part 41.
Department of Treasury—–Office of Thrift Supervision—12 C.F.R. Part 571.
Federal Deposit Insurance Corporation—12 C.F.R. Parts 334 and 364.
Federal Register—Identity Theft Red Flags and Address Discrepancy under the Fair and Accurate Credit Transactions Act of 2003, Part IV.
Federal Reserve System—12 C.F.R. Part 222.
Federal Trade Commission—16 C.F.R. Part 681.
National Credit Union Administration—12 C.F.R. Part 717.

Homeland Security

A volume in the series *Center for National Threat Assessment*

Sensitive security information (SSI) is a category of sensitive but unclassified information under the United States government's information sharing and control rules. SSI plays a crucial role in all types of security. It is information obtained in the conduct of security activities which, if publicly disclosed, would constitute an unwarranted invasion of privacy, reveal trade secrets, share privileged or confidential information, harm transportation security, or allow hostile elements to avoid security controls.

Divided into seven sections, the **Sensitive Security Information, Certified® (SSI) Body of Knowledge** provides a comprehensive source that helps you prepare for certification in SSI protection. It reviews and discusses relevant topics in

- The history and definition of SSI
- Espionage, security breaches, and detection
- Personal information security
- Corporate security
- Government security
- Legislation and regulations
- Identity theft

Within the sections, the book covers a wide range of subjects related to aiding protection of SSI, including

- Good information practices
- The psychology of spies
- Methods to detect potential betrayal
- Methods for handling sensitive information
- Establishing security plans for sensitive information
- Monitoring techniques such as the use of closed-circuit video cameras

In a world of ever-changing technology with massive amounts of information available to the public in a matter of seconds, government, businesses, and individuals must take extra precautions in securing their SSI. This book equips you with the essential knowledge to become certified in SSI protection, and will serve as a valuable reference afterward in remaining an effective security professional charged with protecting SSI.

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K27288
ISBN: 978-1-4987-5211-4
90000
9 781498 752114

www.crcpress.com